



Proposal and Evaluation of Authentication Protocols for Smart Grid Networks

Luis Fernando Arias Roman

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

**FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA**

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA
ELÉTRICA

**Proposal and Evaluation of Authentication
Protocols for Smart Grid Networks**

Luis Fernando Arias Roman

Orientador: Paulo Roberto de Lira Gondim

Banca Examinadora

Prof. Paulo Roberto Gondim, UnB/ ENE (Orientador) _____

Prof. Joel José Puga Coelho Rodrigues, INATEL _____

Prof. Paulo Henrique Portela De Carvalho, UnB/ ENE _____

Prof _____

**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**PROPOSAL AND EVALUATION OF AUTHENTICATION
PROTOCOLS FOR SMART GRID NETWORKS**

LUIS FERNANDO ARIAS ROMAN

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:



PAULO ROBERTO DE LIRA GONDIM, Dr., ENE/UNB
(ORIENTADOR)



PAULO HENRIQUE PORTELA DE CARVALHO, Dr., ENE/UNB
(EXAMINADOR INTERNO)



JOEL JOSÉ FUGA COELHO RODRIGUES, Dr., INATEL
(EXAMINADOR EXTERNO)

Brasília, 23 de fevereiro de 2018.

FICHA CATALOGRÁFICA

Arias Roman, Luis Fernando

AAR696p Proposal and Evaluation of Authentication Protocols for Smart Grid Networks
/ Luis Fernando Arias Roman; orientador Paulo Roberto Gondim.
-- Brasília, 2018. 123 p.

Dissertação (Mestrado - Mestrado em Engenharia Elétrica)
- Universidade de Brasília, 2018.

- | | |
|-------------------------------|-------------------------------------|
| 1. Protocolo de Autenticação. | 2. Smart Grid |
| 3. Vehicle to Grid | 4. Advanced Metering Infrastructure |

I. Gondim, Paulo Roberto, orient. II. Título.

REFERÊNCIA BIBLIOGRÁFICA

ARIAS ROMAN, L. F. (2016). Proposal and Evaluation of Authentication Protocols for Smart Grid Networks. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGEE.DM – 688/2018, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 123p.

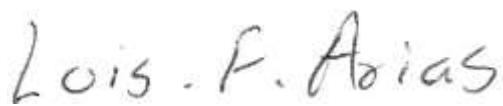
CESSÃO DE DEREITOS

AUTOR: Luis Fernando Arias Roman,

TÍTULO: “Proposal and Evaluation of Authentication Protocols for Smart Grid Networks”.

GRAU/ANO: Mestre/2018

É concedida á Universidade de Brasília permissão para reproduzir cópias desta dissertação de mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte dessa dissertação de mestrado pode ser reproduzida sem autorização por escrito do autor.



Luis Fernando Arias Roman
UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.
709-900 – Brasília – DF – Brasil.

Agradecimentos

A minha esposa Dianita Moon por toda a sua compreensão, apoio e especialmente pelo amor que me ajudou a lidar com os momentos difíceis e curtir as maravilhas deste país junto a minhas cachorrinhas “Luly” e “Campanita”.

A minha mãe por ser uma mulher que me ensinou a ser forte e perseverar para alcançar meus objetivos e um exemplo de vida. A meus sogros pela torcida e o carinho.

A meus irmãos e sobrinho, que me ofereceram todo seu amor e apoio, a meus tios e primos que são minha fortaleza e o exemplo a seguir. Ao meu pai, pelos conselhos e apoio.

A meu orientador Paulo Gondim, pela paciência, conselhos, o apoio e por acreditar no meu esforço e trabalho no mestrado, com ele quiser trabalhar e aprender por muito tempo mais. Ao professor Jaime Lloret pelo apoio no trabalho desenvolvido.

Aos meus amigos no Brasil Bety, Harry, Andres, Tatiana, Noel, Yarisley, Rogerio, dona Francisca e Pedro, pela torcida e amizade.

Aos meus melhores Amigos Daniel, Carlos, Guevarita, El Pastusito e Carlos Mario pela companhia e sua boa energia, eles nunca estão longe.

Aos meus amigos mais estimados na Colômbia, as Angelitas, os Carlitos, Pipe e Andres, pela torcida e apoio.

Ao pessoal do Laboratório de Televisão Digital da UnB e ao Programa de Pós-graduação em Engenharia Elétrica da UnB.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pela bolsa de estudos.

Resumo

Uma rede *Smart Grid* (ou rede elétrica inteligente) representa a evolução das redes elétricas tradicionais, tornada possível graças à integração das tecnologias da informação e das comunicações com a infraestrutura elétrica. Esta integração propicia o surgimento de novos serviços, tornando a rede elétrica mais eficiente, gerando também novos desafios a serem atendidos, dentre eles a segurança do sistema.

A rede SG deve garantir a confiabilidade, a integridade e a privacidade dos dados armazenados ou em trânsito pelo sistema, o que leva à necessidade de autenticação e controle de acesso, obrigando a todo usuário ou dispositivo a se autenticar e a realizar somente operações autorizadas.

A autenticação de usuários e dispositivos é um processo muito importante para a rede SG, e os protocolos usados para esse fim devem ser capazes de proteção contra possíveis ataques (por exemplo, *Man-in-the-Middle* - MITM, repetição, Denegação de Serviço - DoS). Por outro lado, a autorização é tratada em conjunto com a autenticação e relacionada com as políticas de controle de acesso do sistema.

Uma parte essencial para criar os protocolos de autenticação seguros envolve os esquemas de ciframento. O uso de um ou a combinação de vários esquemas afeta diretamente o desempenho do protocolo. Cada dia novos esquemas são propostos, e seu emprego nos protocolos de autenticação melhora o desempenho do sistema em comparação aos protocolos já propostos no mesmo cenário.

Neste trabalho são propostos 3 (três) protocolos de autenticação seguros e de custo adequado para os cenários descritos a seguir:

- Autenticação dos empregados das empresas de fornecimento de energia que procuram acesso ao sistema de forma remota;
- Autenticação de *Smart Meters* numa Infraestrutura de medição avançada (AMI, do inglês *Advanced Metering Infrastructure*) baseada em nuvem computacional; e
- Autenticação de veículos elétricos em uma rede V2G (do inglês, *Vehicle-to-Grid*).

Cada um dos cenários tem características particulares que são refletidas no projeto dos protocolos propostos. Além disso, todos os protocolos propostos neste trabalho garantem a autenticação mútua entre todas as entidades e a proteção da privacidade, confidencialidade e integridade dos dados do sistema.

Uma comparação dos custos de comunicação e computação é apresentada entre os protocolos propostos neste trabalho e protocolos desenvolvidos por outros autores para cada um dos cenários. Os resultados das comparações mostram que os protocolos propostos neste trabalho têm, na maioria dos casos, o melhor desempenho computacional e de comunicações, sendo assim uma ótima escolha para a sua implementação nas redes SG.

A validação formal dos protocolos propostos por meio da ferramenta AVISPA é realizada, permitindo verificar o atendimento a requisitos de segurança.

Palavras-chave – *Smart Grid (SG), Vehicle to Grid (V2G), Infraestrutura de medição Avançada (AMI), Chave de Sessão, Protocolo de Autenticação, Confidencialidade, Privacidade, AVISPA.*

Abstract

A Smart Grid network (or intelligent electrical network) represents the evolution of traditional electrical networks, made possible due to the integration of information and communication technologies with the electrical power grid. This integration generates new services and improves the efficiency of the electrical power grid, while new challenges appear and must be solved, including the security of the system.

The SG network must assure reliability, integrity and privacy of the data stored or in transit in the system, leading to the need for authentication and access control, thus all users and devices must authenticate and accomplish only authorized operations.

The authentication of users and devices is a very important process for the SG network, and the protocols used for this task must be able to protect against possible attacks (for example, Man-in-the-Middle - MITM, repetição, Denegação de Serviço – DoS). On the other hand, authorization is treated jointly with authentication and related to policies of access control to the system.

An essential part of creating secure authentication protocols involves encryption schemes. The use of one or the combination of several schemes directly affects protocol performance. Each day new schemas are proposed, and their utilization in the authentication protocols improves the performance of the system compared to the protocols already proposed in the same scenario.

In this work 3 (three) secure and cost-effective authentication protocols are proposed, for the following scenarios:

- Authentication of employees of energy supply enterprises, looking for remote or local access to the system;
- Authentication of Smart Meters in an Advanced Metering Infrastructure based on cloud computing; and
- Authentication of electrical vehicles in a V2G (“Vehicle-to-Grid”) network.

Each scenario has specific characteristics, that are reflected on the design of the proposed protocols. Moreover, such protocols assure mutual authentication among entities as well as the protection of privacy, confidentiality and integrity of system data.

A comparison considering communication and computing costs is presented, involving proposed protocols and other previously published protocols, for each scenario. The results show that the proposed protocols have, in most cases, the best performance, thus constituting good choices for future implementation in SG networks.

The formal validation of the proposed protocols by the use of AVISPA tool is realized, allowing to verify the compliance with security requirements.

Keywords – Smart Grid (SG), Vehicle to Grid (V2G), Advance Metering Infrastructure(AMI), Session Key, Authentication Protocol, Confidentiality, Privacy, AVISPA.

Table of Contents

1. Chapter 1	15
INTRODUCTION.....	15
1.1. Initial Considerations.....	15
1.2. Motivation.....	16
1.3. Objectives.....	17
1.4. Methodology.....	18
1.5. Contributions.....	18
1.6. Organization	19
1.7. References.....	20
2. Chapter 2	21
THEORETICAL BACKGROUND	21
2.1. Preliminary Definitions.....	21
2.2. Security Attacks.....	22
2.2.1. Passive Attacks	22
2.2.2. Active Attacks.....	22
2.3. Models of Cryptography and Key Agreement.....	23
2.3.1. Symmetric Cipher Model.....	23
2.3.2. Asymmetric Cipher Model.....	23
2.3.3. Diffie-Hellman Key Exchange	25
2.4. Authentication.....	26
2.5. Access Control	26
2.6. Schemes of Ciphering.....	27
2.7. Smart Grid Architecture	28
2.7.1. Architecture of Smart Grid	28
2.7.2. Smart Grid Communications Architecture	30
2.8. AVISPA Tools	32
2.9. References.....	34
3. Chapter 3	37
Authentication and RABAC-Based Access Control Protocol for Smart Grids.....	37
3.1. Introduction	37
3.2. Related Work.....	38
3.3. System Model.....	39

3.4.	Adversary Model	40
3.5.	Proposed Protocol.....	41
3.6.	Analyses of Security and Performance.....	47
3.6.1.	Analysis of Security.....	47
3.6.2.	Formal Verification of the Proposed Protocol	49
3.6.3.	Intruder simulation with SPAN.....	52
3.6.4.	Analysis of Performance.....	53
3.7.	Conclusions and Future Work	56
3.8.	References.....	57
4.	Chapter 4.....	59
	Authentication and Authorization Protocol Based on Cloud for Advanced Metering Infrastructure in SG	59
4.1.	Introduction	59
4.2.	Related Work.....	61
4.2.1.	Integration of SG and Cloud	61
4.2.2.	Key Management and Device Authentication in the AMI Network.....	61
4.3.	System Model.....	62
4.4.	Adversary Model	63
4.5.	Proposed Protocol.....	64
4.6.	Security Analysis.....	72
4.7.	Formal Verification of the Proposed Protocol	73
4.7.1.	Protocol Simulation	73
4.7.2.	Results of Security Verification	75
4.7.3.	Simulation of intrusion with SPAN	76
4.8.	Performance Evaluation.....	79
4.8.1.	Communication Cost	79
4.8.2.	Computational Cost.....	80
4.9.	Conclusions and Future Work	82
4.10.	References.....	84
5.	Chapter 5.....	86
	Authentication Protocol for Vehicle to Grid Networks in Smart Grid.....	86
5.1.	Introduction	86
5.2.	Related Work.....	87
5.3.	System Model.....	89

5.4.	Adversary Model.....	90
5.5.	Proposed Protocol.....	91
5.6.	Security and Performance Analyses.....	98
5.6.1.	Security Analysis.....	98
5.6.2.	Formal Verification of the Proposed Protocol.	99
5.6.3.	Simulation of intrusion with SPAN	103
5.6.4.	Performance Analysis.....	105
5.7.	Conclusions and Future Work	110
5.8.	References.....	112
6.	Chapter 6.....	114
	Conclusion.....	114
	APPENDIX I - Letter of Acceptance of article at the XXXV SBRC 2017. O Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2017)	117
	APPENDIX II – Paper “Protocolo de Autenticação e Autorização em “Smart Grids” para Cidades Inteligentes”. Submitted at the Event (SBRC 2017)	118

List of Figures

FIGURE 2.1- MODEL OF SYMMETRIC CRYPTOSYSTEM [3]	23
FIGURE 2.2- PUBLIC-KEY CRYPTOGRAPHY [3].....	24
FIGURE 2.3- PUBLIC-KEY CRYPTOSYSTEM: AUTHENTICATION AND SECRECY[3].....	25
FIGURE 2.4- SMART GRID ARCHITECTURE.....	29
FIGURE 2.5- SEGMENTS OF THE SMART GRID.....	31
FIGURE 3.1- ARCHITECTURE OF A SMART GRID SYSTEM	40
FIGURE 3.2- GENERAL SCHEME OF THE PROPOSED PROTOCOL	41
FIGURE 3.3 PHASES OF PROPOSED PROTOCOL.....	42
FIGURE 3.4- USER’S REGISTRATION PHASE	44
FIGURE 3.5- DEVICE REGISTRATION PHASE.....	44
FIGURE 3.6- ACCESS CONTROL PHASE FOR REMOTE USERS	46
FIGURE 3.7- ACCESS CONTROL PHASE FOR LOCAL USERS.....	47
FIGURE 3.8- USER’S ROLE IN HLSPL	50
FIGURE 3.9- SPECIFICATION OF THE SESSION ROLE IN HLSPL	50
FIGURE 3.10- SECURITY OBJECTIVES OF THE PROTOCOL IN HLSPL	51
FIGURE 3.11- RESULTS OF AVISPA SECURITY SIMULATION	51
FIGURE 3.12- INTRUDER SIMULATION WITH SPAN	52
FIGURE 3.13- COMMUNICATION COSTS OF THE PROTOCOLS	54
FIGURE 3.14- COMPARISON OF COMPUTATIONAL COSTS BETWEEN PROTOCOLS	56
FIGURE 4.1- PROPOSED ARCHITECTURE OF AMI IN THE CLOUD.....	63
FIGURE 4.2 GENERAL SCHEME OF THE PROPOSED PROTOCOL.	64
FIGURE 4.3- PHASES AND FUNCTIONING OF THE PROTOCOL.....	65
FIGURE 4.4- BINARY TREE FOR GROUP ORGANIZATION (SOURCE: [12]).	65
FIGURE 4.5- REGISTRATION PHASE	67
FIGURE 4.6 – BINARY TREE AFTER THE ENTRANCE OF CSP (SOURCE [12]).	70
FIGURE 4.7- AUTHENTICATION PHASE	71
FIGURE 4.9- ROLE SPECIFICATION FOR THE SESSION AND ENVIRONMENT IN HLSPL.....	74
FIGURE 4.10- SECURITY GOALS ESTABLISHED IN HLSPL	75
FIGURE 4.11- RESULTS OF A SECURITY SIMULATION FOR OFMC AND CL-ATSE.....	76
FIGURE 4.12- INTRUSION SIMULATION BETWEEN SM AND AG WITH SPAN	77
FIGURE 4.13- INTRUSION SIMULATION BETWEEN AG AND CSP WITH SPAN.....	78
FIGURE 4.14- COMMUNICATION COSTS OF THE PROTOCOLS	80
FIGURE 4.15- COMPARISON OF COMPUTATIONAL COSTS AMONG THE PROTOCOLS.....	82
FIGURE 5.1- ARCHITECTURE OF A V2G NETWORK	90
FIGURE 5.2- GENERAL SCHEME OF THE PROPOSED PROTOCOL.	91
FIGURE 5.3- PHASES OF THE PROPOSED PROTOCOL	92
FIGURE 5.4- REGISTRATION PHASE	93
FIGURE 5.5- AUTHENTICATION PHASE.....	97
FIGURE 5.6- ROLE OF EV IN HLSPL.....	100
FIGURE 5.7- SPECIFICATION OF THE ROLE OF SESSION IN HLSPL.....	101
FIGURE 5.8- SECURITY OBJECTIVES AND RELATED SECRETS OF THE PROPOSED PROTOCOL IN HLSPL ..	102
FIGURE 5.9- SECURITY SIMULATION RESULTS FOR OFMC AND CL-ATSE	102
FIGURE 5.10 INTRUSION SIMULATION BETWEEN EV AND AG WITH SPAN.....	103
FIGURE 5.11- INTRUSION SIMULATION BETWEEN AG AND SAS WITH SPAN.....	104
FIGURE 5.12- COMMUNICATION COSTS OF THE PROTOCOLS	106
FIGURE 5.13- COMPARISON OF COMPUTATIONAL COSTS AMONG PROTOCOLS.....	108
FIGURE 5.14- COMPUTATIONAL COST IN REGISTRATION AND AUTHENTICATION PHASES, FOR ENTITIES OF THE PROPOSED.....	109
FIGURE 5.15- STORAGE COST OF THE PROTOCOLS.....	110

List of Tables

TABLE 3.1- SYMBOLS AND COST IN BITS (SAXENA ET AL. [7]).	43
TABLE 3.2- SECURITY ANALYSIS OF THE PROTOCOLS.	49
TABLE 3.3- COMPARISON OF COMMUNICATION COSTS	54
TABLE 3.4- OPERATIONS AND TIME COSTS	55
TABLE 3.5. COMPARISON OF COMPUTATIONAL COSTS.	55
TABLE 4.1- AUTHENTICATION VARIABLES	66
TABLE 4.2- PRIVATE / PUBLIC KEYS.	67
TABLE 4.5- SESSION KEY GENERATION	71
TABLE 4.6- COMMUNICATION COST OF EACH PARAMETER TRANSMITTED [13].	79
TABLE 4.7- COMMUNICATION COSTS IN BITS PER MESSAGE AND TOTAL.	79
TABLE 4.8- NOMENCLATURE USED AND TIME SPENT ON EACH OPERATION [3].	81
TABLE 4.9- COMPARISON OF THE COMPUTATIONAL COSTS OF THE PROTOCOLS FOR THE GENERATION AND DISTRIBUTION OF KEYS IN THE DEVICES.	81
TABLE 5.1- CALCULATION OF VALUES FOR A BROADCAST MESSAGE.	95
TABLE 5.2- CALCULATION OF THE SAS SESSION KEYS.	95
TABLE 5.3- CALCULATION OF EVS AND AG SESSION KEYS.	96
TABLE 5.4- COMPARISONS OF ENTITIES OF THE V2G ARCHITECTURE	98
TABLE 5.5- SYMBOLS AND COST IN BITS [13].	105
TABLE 5.6- COMMUNICATION COST IN BITS PER MESSAGE	106
TABLE 5.7- COST IN MS OF EACH OPERATION AND ENTITY CONSIDERED [19].	107
TABLE 5.8- COMPUTATIONAL COST OF THE AUTHENTICATION PHASE	107
TABLE 5.9- STORAGE COST OF THE AUTHENTICATION PHASE	109

Abbreviations

ABAC	Attribute-Based Access Control
AG	Aggregator
AMI	Advanced Metering Infrastructure
AVISPA	Automated Validation of Internet Security Protocols and Applications
BS	Backward Secrecy
CAS	Central Authentication Server
CC	Control Center
CL-AtSe	Constraint Logic-based Attack Searcher
CSP	Cloud Solution Provider
DoS	Denial of Service
EV	Electric Vehicle
FS	Forward Secrecy
GKi	Group Key of group i
HLPSL	High Level Protocol Specification Language
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IoT	Internet of Things
LAG	Local Aggregator
MAC	Message Authentication Code
MitM	Man-in-the-Middle
Ms	Milliseconds
NIST	National Institute of Standards and Technology
OFMC	Open-source Fixed-point Model Checker
PBC	Pairing-based cryptography
PEV	Plug-In Electric Vehicle
PFP	Permission Filtering Policy

RBAC	Role-Based Access Control
RABAC	Role-Centric Attribute-Based Access Control
SAS	Substation Authentication Server
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SM	Smart Metering
TA	Trusted Authority
V2G	Vehicle to Grid

Chapter 1

INTRODUCTION

1.1. Initial Considerations

An Smart Grid (SG) network is a proposal that is transforming the paradigm of generation, transportation, distribution and consumption of electric energy, considering that the traditional electrical power system had a low integration with the information technologies that allowed the communication of only the substations and the control centers. SG is expected to be a key part of the power grid, allowing a large number of electrical devices to be controlled and monitored remotely, thus achieving a more automated, intelligent and efficient network [1].

The Smart grid represents the next-generation cyber-physical network, where the concepts of physical electricity network and the cybernetic network of communications are mixed, providing communication with a private network or the internet [6].

The National Institute of Standards and Technology (NIST) created a conceptual model of SG. NIST divides the model into seven domains communicating between them to harmonize SG dynamics [2]. Below are described the domains:

- Power generation domain: This is formed by power plants. To generate a balance in the supply and demand of energy, this domain must communicate with the domains of operation and the market domain;
- Consumer domain: This is formed by the end users who consume, produce and store energy that can be sold to the public power grid. This domain must communicate with the operations domain;
- Transmission domain: This is conformed by the transmission substations and the network of wires that carry the energy from the generating plant to it.
- Distribution domain: the distribution system is the network that transports the energy from the distribution substation to the houses, this domain has to communicate with the operations domain;
- Domain of service providers: it is the entity that manages the energy consumption of users, this domain has to communicate with the market domain and the domain of operation;
- Domain of the energy market (wholesale, retail and commerce): this domain is responsible for balancing the supply and demand of energy, therefore it has to communicate with the domains of generation, providers and operation of the electricity network;
- Domain of the electric network operation: it is responsible for collecting data to ensure control and efficient operation of the system.

Communications are fundamental for the SG to have control over the stabilization of demand, management of charging, purchase and sale of energy to end consumers, and it is necessary that the communications infrastructure and related applications have a high level of protection and reliability.

A challenging security issue facing the SG system is the lack of mutual authentication between reported entities, the risk of multiple cyber attacks, unauthorized access to resources, and so on. The consequence of these security problems is the compromise of information exchanged between entities, for example, causing unauthorized data modification, generating network latency and possibly exposing customer information.

The SG network is responsible for the availability of information, as well as ensuring the confidentiality and privacy of data, and the protection of message integrity. The SG network

to comply with these responsibilities must have a network access control, so it must authenticate and authorize any access attempts of devices or users.

Authentication is a process of verifying the identity of a device or user, so authorization is the process of checking the permissions that a device or user has to perform actions on the system. Authentication is a very important research topic in SG network communications because some protocols implemented in the system are vulnerable to various attacks such as Man-in-the-Middle (MITM), impersonation, repetition and proxy attacks, and so on [3]. Authorization is a topic commonly treated in a joint manner with authentication (4-5), and is closely related to access control policies.

Many researchers are actively working on building secure and efficient authentication protocols to solve various communication, security, and privacy challenges in different scenarios of SG networks. Such scenarios involve the need for authentication protocols, that are required for authenticating:

- employees of energy supply companies and vendors;
- devices of Advanced Measurement Infrastructure (AMI); and
- electric vehicles (EV) or Plug-In EV (PEV) in Vehicular-to-Grid (V2G) networks.

Each of these scenarios of SG networks has its unique characteristics that makes the task of creating protocols a complex task. In the case of authentication of people working on energy suppliers, it must be taken into account that there are several types of employees with different roles and attributes within the company, therefore it is necessary that the access to resources is granted in a specific way for each user, according his/her roles and attributes. In this way, only authenticated users must be able to perform the duly authorized actions on the devices and other resources.

In the case of AMI device authentication, it must be taken into account that the AMI network is composed of several entities with different computing and communication capacities; in addition, due to the exponential growth in the number of devices and their high availability characteristics, authentication schemes must be able to support the authentication of large numbers of devices and ensure protection against several attacks (Denial of Service (DoS), Man-in-the-Middle (MITM), impersonation and repetition attacks, for example).

In the case of authentication of electric vehicles (EV) in the V2G network, it must take into account the mobility and geographical location of the vehicle, loading and unloading operations, driving pattern, among others. In the V2G network, special attention should be paid to information classified as confidential: vehicle identity, user identity, identification of the loading station, type of vehicle, loading and unloading time, vehicle location.

Thus, regardless of the scenarios, authentication protocols should provide an efficient and secure communication environment that ensures mutual authentication between all entities and privacy protection.

1.2. Motivation

Motivations for the research and development in this area involve, initially, obsolescence of infrastructure of electrical power system and improvements in reliability, security and energetic efficiency. Moreover, SG's also constitute a pillar for the possible implantation of smart cities and use of electric or hybrid vehicles.

The SG network is responsible for the security of the user data that is transported by the SG network, so it must be ensured that the data can only be accessed by authorized personnel or

equipment, this can be achieved through the implementation of authentication protocols and access control for the devices or users of the SG network.

In terms of standards, there are some standardized protocols in the literature for SG such as the OpenADR for the demand response program and the IEC 62056 standard for the AMI network, which is the product of the mixing of an application layer communication protocol called Device Language Message Specification (DLMS) and a data model called the companion specification for energy metering (COSEM). The DLMS and COSEM uses three authentication procedures that are restricted to encryption of symmetric keys: non-security (public access without identity verification), low-level security authentication (the server identifies the client by password), and high security authentication level (mutual identification) with exchange of challenges. On the other hand OpenADR makes authentication based on public key cryptography with certificate exchange, in its architecture a hierarchy of certified authorities is modeled and it needs a PKI to use in three layers, which results in high computational cost and communications [3].

On the other hand, the good performance of the protocols used in SG is very important to satisfy the requirements of the service. Specifically, we observe that SG network authentication protocols have proper characteristics of data confidentiality and privacy that the current standard protocols are not serving, so the academic community is developing new protocols that comply with most or all security features.

The architectures considered in the SG networks and encryption schemes are fundamental part of the authentication protocols, possibilitating to define the behavior of the protocols: messages exchanged between devices, number of and bits per message, operations to execute in each device, among others. The use of an encryption scheme or a mixture of several ones can lead to good results, thus reducing communication costs and computational costs.

Therefore, there is a motivation to develop new authentication protocols based on new encryption schemes or the mixture of several ones, seeking to satisfy all the security requirements of SG networks, with good or very good communication and computational costs, and scalability to support the growing number of devices that are part of the SG network.

1.3. Objectives

General objective:

To propose authentication and authorization protocols in different scenarios of the SG networks, which preserve information security and perform well in comparison to other protocols already published.

Specific objectives:

- 1- Identify and apply basic and advanced concepts regarding new techniques of protection, mainly related to confidentiality, privacy and integrity, as well as, secondarily, non-repudiation and availability in SG networks;
- 2 - Evaluate different proposals of authentication protocols based on 3 different scenarios of SG networks, for further comparison;
- 3- Characterize and evaluate different key data encryption and management schemes.
- 4- Propose authentication protocols in 3 different scenarios of SG networks, with a good performance;
- 5- Validate the protocols proposed in the research by using formal security verification techniques.

1.4. Methodology

The methodology adopted in the research considers the following phases:

- Phase 1: general bibliographic review on the topic;
- Phase 2: an in-depth study about SG security;
- Phase 3: in-depth study on authentication protocols in the SG;
- Phase 4: in-depth study on encryption, authentication and key agreement schemes;
- Phase 5: proposal of security protection protocols that meet necessary security, computational and communications efficiency requirements, considering three different scenarios;
- Phase 6: formal validations of proposed protocols;
- Phase 7: dissertation writing and defense.

The proposed protocols focus mainly on authentication, authorization and key agreement issues. Considering a general architecture of a SG system, three scenarios were treated:

- Access control and management of equipments and other resources of the electricity network by the employees of the energy supply company;
- In the acquisition of measurement data in the AMI architecture;
- Access to the service of the V2G network by the electric vehicles.

For each scenario, a set of entities was considered, served by a given infrastructure of communication. Some premises/assumptions related to possible insecure parts were adopted. Then, considering possible threats and vulnerabilities, a set of security properties was considered as objectives to be reached by the proposed protocols.

For the sake of comparisons among protocols, communication costs were evaluated, considering message flows and bandwidth consumption; additionally, computing costs were also evaluated, considering processing times of operations made by the protocols.

Finally, formal validation of the proposed protocols was accomplished, using a tool named AVISPA as well as some of the respective back-ends and a graphical animator.

1.5. Contributions

The following contributions can be highlighted:

- Survey and discussion about the proposed authentication protocols for SG networks;
- Proposal of an authentication and access control protocol for a scenario of control and management of the electricity network equipment by the employees of the energy supply company;
- Proposal of an authentication protocol for a scenario of acquisition of measurement data in the AMI architecture, integrated to the cloud;
- Proposal of an authentication protocol for a scenario of access to the V2G network service by plug-in electric vehicles;
- Evaluation of the performance of the proposed protocols, in terms of communication and computational costs;
- Formal validation of the proposed protocols.

1.6. Organization

The remainder of this dissertation is organized as follows: Chapter 2 presents security related concepts and authentication schemes, as well as the SG network architecture considered for the development of the proposed protocols.

In Chapter 3, protocols devoted to the authentication of users (employees) of a power supply company and the SG network are presented, followed by a proposed protocol that performs dynamic authorization for each user based on its role and respective attributes, using bilinear pairing and some concepts and techniques present in the Certificate-Based Signcryption (CBS) [Li 2008] cryptographic system.

Chapter 4 presents protocols related to authentication and key management in a cloud-based AMI architecture, followed by the second protocol, that uses a binary tree structure for group management as well as Certificate-Based Signcryption (CBS) and bilinear pairing to provide efficient authentication of a group of devices.

Chapter 5 presents protocols related to group authentication for the administration and distribution of keys in a V2G architecture, followed by the third proposed protocol, using Elliptic Curve Diffie Hellman (ECDH) for sharing secrets and bilinear pairing to provide authentication and generation of simultaneous and efficient session keys for EVs grouped in aggregators.

Finally, Chapter 6 presents the conclusions of the work developed and the proposals of future work for the continuity of this dissertation.

1.7. References

- [1] Y. Lopes, T. Bornia, V. Farias, N. C. Fernandes, D. C. Muchaluat-Saade “Desafios de Segurança e Confiabilidade na Comunicação para Smart Grids”, XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Minicurso Smart Grid, 2016.
- [2] National Institute of Standards and Technology (NIST), “G NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0”, NIST Special Publication 1108r3, 2014
- [3] N. Saxena, B. J. Choi, “State of the Art Authentication, Access Control, and Secure Integration in Smart Grid”, *Energies*, vol. 8 Issue 10, pp. 11883-11915, 2015.
- [4] Vaidya, B., Makrakis, D., and Mouftah, H.(2013) “Authentication and Authorization Mechanisms for Substation Automation in Smart Grid Network”. *IEEE Network*, v.27, P. 5-11, 2013.
- [5] N. Saxena, B. Choi, B. Lu, “Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid”. *IEEE Transactions On Information Forensics And Security*. v.11, 2016.
- [6] Y. Simmhan, S. Aman, A. Kumbhare, R. Liu, S. Stevens, Q. Zhou, V. Prasanna “ Cloud-Based Software Platform for Big Data Analytics in Smart Grids”, *Computing in Science & Engineering* , vol. 15, pp. 38-47, 2013.

Chapter 2

THEORETICAL BACKGROUND

***Abstract:** This chapter provides the necessary concepts to understand the protocols proposed in this work such as authentication, access control, encryption schemes, and a description of the architecture and the components of a Smart Grid. A discussion of security problems in SG, specially on authentication, access control and key management is presented. In the final part, some discussion about validation of protocols is provided.*

2.1.Preliminary Definitions

The following were the formal definitions of computer security made in publications recognized and accepted by the entire academic community. In [1] the computer security is defined as:

- **Computer Security Concepts:**

“Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated”.

Of the previous definition arise three principals objectives of the computer security, called CIA triad, product of the acronym confidentiality, integrity and availability. In [2] a definition of the three terms is given:

- **Confidentiality**

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information”.

- **Integrity:**

“Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information”.

- **Availability:**

“Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system”.

In addition to the Triad, Stallings makes an important characterization of the term Authenticity that is needed to understand the security objectives.

- **Authenticity :**

“The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.” [3]

In ITU-T Recommendation X.800, Security Architecture for OSI, three concepts widely used in the field of information security are clearly defined [4].

- **Security attack**

“Any action that compromises the security of information owned by an organization” [4].

- **Security mechanisms**

“A security policy may be implemented using various mechanisms, singly or in combination, depending on the policy objectives and the mechanisms used. In general, a mechanism will belong to one of three (overlapping) classes: a) prevention; b) detection; and c) recovery. Security mechanisms appropriate to a data communications environment are discussed below” [4].

- **security service**

“A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers” [4].

In addition to RFC 4949, Internet Security Glossary, the concepts of Threat and Attack are differentiated.

- **Threat**

“A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability” [5].

- **Attack**

“An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system” [5].

2.2.Security Attacks

Security attacks are classified into two active and passive types, depending on their interaction the attacker with the target system.

2.2.1.Passive Attacks

The purpose of this type of attack is to spy or to monitor the transmitted information by making a release of message contents or a traffic analysis [Stallings].

- **Release of message contents**

Is when an attacker discovers contents of sensitive or confidential transmissions.

- **Traffic analysis**

By analyzing the flow of messages between two interlocutors and with the help of techniques and tools, an attacker could visualize the data even if they are encrypted.

2.2.2. Active Attacks

The purpose of such attacks is to modify a data stream or create a false data stream. this attack is classified into four categories: masquerade, replay, modification of messages, and denial of service[3].

- **Masquerade:** occurs when an entity created by the attacker pretends to be another entity to pick up their system privileges.

- **Replay:** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

- **Modification of messages:** is when a part of a valid message is changed.

- **Denial of service:** is when an attacker can block a service supported on a computer.

2.3.Models of Cryptgraphy and Key Agreement

2.3.1.Symmetric Cipher Model

In the symmetric encryption model it is necessary that the sender and receiver have the same secret key and execute the same encryption / decryption algorithm.

Figure 2.1 shows the model of a symmetric cryptosystem. When a sender wants to securely send a message with clear text X data to the remote destination via an insecure communication channel, the promising thing to do is to gear an encryption key K . With this key and an encryption algorithm, clear text message X in an encrypted message $Y = E(K, X)$, where E is the encryption algorithm. once the message has been encrypted is sent to the destination and in parallel via a secure channel, sends the encryption key K to the receiver. When the message Y arrives at the destination, the receiver makes use of the received K key and a deciphering algorithm to obtain the original $X = D(K, Y)$ message, where D is the decryption algorithm.

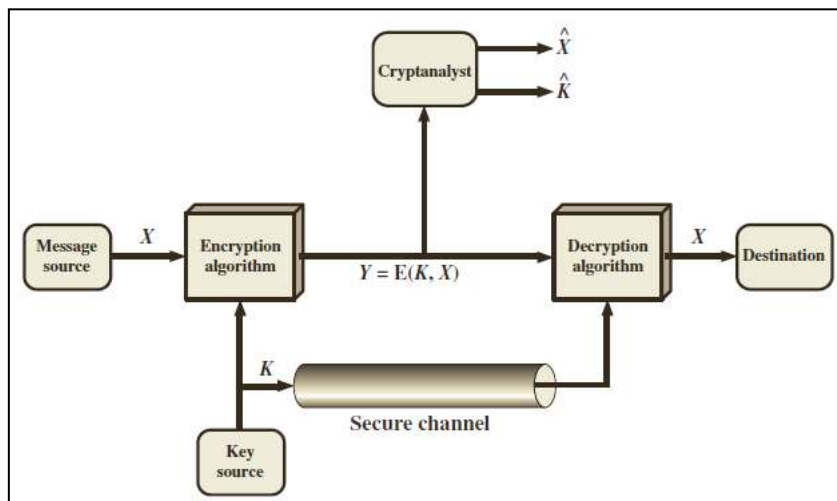


Figure 2.1- Model of Symmetric Cryptosystem [3]

If an attacker is interested in message X , he picks up the message Y , and with the aid of tools and tools, he has generated an estimate of the clear text X . If the attacker is interested in reading all the messages sent to the receiver, he picks up the message Y and tries to find the key K .

2.3.2. Asymmetric Cipher Model

The most important system of asymmetric encryption models are public key crypto systems that have different keys to encrypt and decrypt a message.

Figure 2.a shows the public key encryption scheme that has five elements and describes the process of sending a message from Bob to Alice:

- i. Clear text: message X with readable data to send.
- ii. Encryption Algorithm (E): performs transformations of light text X in a ciphertext Y .
- iii. Encrypted Text: Encrypted Text Y is the product of the execution of the Encryption Alorith over clear text X by applying a Alice Public Key (PU_a)

- iv. Public and Private Keys: These are a Public (PUa) and Private (PRa) pair of keys selected by Alice, so the public key PUa is known by all and can be used for clear text X's encryption by either persona that wants to send a message to Alice, and the other key PRa is only known to Alice in such a way that along with the decryption algorithm it converts the ciphertext Y sent by Bob to the plaintext X.
- v. Decryption algorithm (D): accepts the ciphertext Y and produces the original clear text.

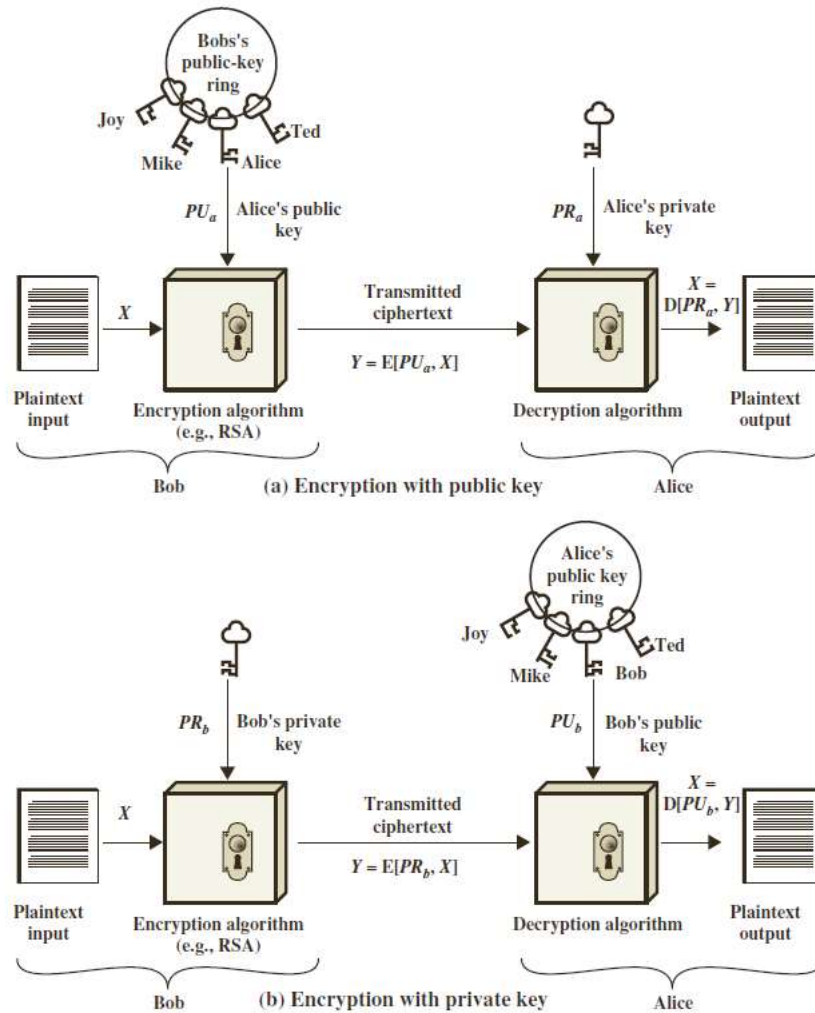


Figure 2.2- Public-Key Cryptography [3]

In the case of figure 2.b, it follows the same steps described for figure 2.a, but it has a great difference, since the encryption of the clear text is made with the private key of Bob (PRb) and sends a message to Alice . When Alice receives the message, she performs the decryption process with Bob's public key (PUb).

The encryption process with the public key of figure 2.a is generally used for the secrecy of the transmitted data, but not for authenticating the sender of the message, since the message was encrypted with the public key which as its name indicates any person was able to encrypt the message and send it. In the encryption process with the private key of figure 2.b, authentication is usually used (digital signature), but not for the secrecy of the message, because when a sender sends an encrypted message with his private key, any person who picks up the message can decipher it , since with public key of the sender is known by all.

In figure 2.3 a solution is shown so that the message X is confidential and authenticated. the first step is to encrypt the message X with the private key PRa of the recipient A, converting

the message X into a message Y so that the recipient B authenticates the identity of the sender A, step two is to encrypt the message Y with the public key PUB of the recipient B, converting the message Y into a message Z, to protect the secrecy of the message.

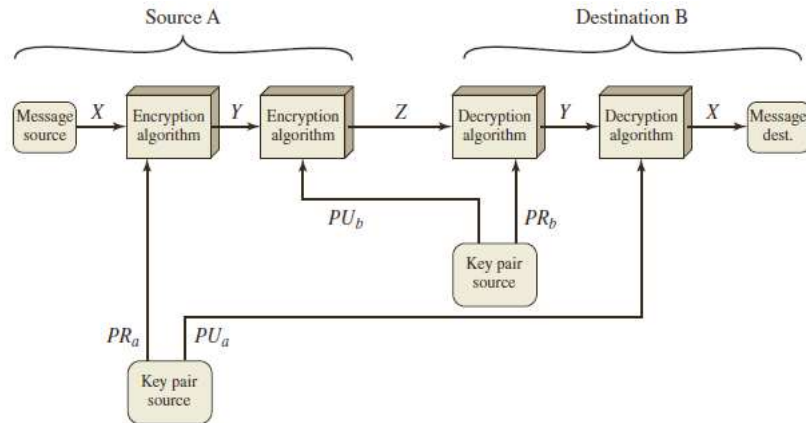


Figure 2.3- Public-Key Cryptosystem: Authentication and Secrecy[3]

2.3.3. Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange algorithm is the first public key algorithm. The purpose of this algorithm is to exchange keys between two users in a secure way. A summary of the Diffie-Hellman key exchange process is shown below. When two users want to share a session key they should follow the following steps:

- i. The two must agree on a sufficiently large prime number q and a primitive root of a , to initialize the system.
- ii. the two users A and B choose a private random envelope X_A and X_B smaller than q
- iii. that will be their keys published respectively, and then each one calculates the public value:
 $Y_A = a^{X_A} ; Y_B = a^{X_B}$ Respectfully.
- iv. The users A and B take the public keys of Y_B and Y_A respectively,
- v. each one does the following calculation to find the shared key: $K_A = (Y_B)^{X_A} \text{ mod } q = K_B = (Y_A)^{X_B} \text{ mod } q$

The following is mathematically demonstrated (using rules of modular arithmetic) that the keys calculated separately by the users are equal:

$$\begin{aligned}
 K &= (Y_B)^{X_A} \text{ mod } q \\
 &= (a^{X_B} \text{ mod } q)^{X_A} \text{ mod } q \\
 &= (a^{X_B})^{X_A} \text{ mod } q \\
 &= a^{X_B X_A} \text{ mod } q \\
 &= (a^{X_A})^{X_B} \text{ mod } q \\
 &= (a^{X_A} \text{ mod } q)^{X_B} \text{ mod } q \\
 &= (Y_A)^{X_B} \text{ mod } q
 \end{aligned}$$

The Security of the Diffie-Hellman Algorithm depends on the discrete logarithm problem (DLP).

2.4. Authentication

Authentication of users and devices is the first line of defense in information technology (IT) security. Users or devices must perform authentication to prove their identity to a system before a session is started. This is referred to as entity authentication. In addition, in some cases additional authentication may be required to authorize some action that needs greater privileges to execute [6][7].

There are four factors for the authentication of people and devices: something that the user or device knows (for example, password or PIN), something that the user or device possesses (for example, a cell phone or token), something that the user or device is (for example, a biometric feature for people and the recognition of digital signatures in the case of machines) and something that the user or device does (for example, speech recognition for the user and the recognition of the Physical Unclonable Function (PUF) for the devices [6].

In systems where entities to communicate switch non-secure channel messaging, advanced encryption schemes are required to prevent unauthorized entities from reading information that is transmitted [8].

2.5. Access Control

The control of access to systems is fundamental for guaranteeing their confidentiality, integrity and availability. Controls can be administrative (entrepreneurial policies), logical (authentication and authorization protocols) or physical (restriction of admission to critical zones through doors). Such control comprises several models, but the following will be described those most cited in the literature:

- Role-Based Access Control (RBAC)

A central authority determines or manages users that can access controlled objects. Authorization is based on their duties, responsibilities, qualifications and role in the organization. Although the administration and audit cost of the model is reduced, it cannot deal with attributes that change dynamically, e.g. hour, location, etc. [9-14].

- Attribute-Based Access Control (ABAC)

It controls users' access through policies developed from the mixing of different attributes classified into 4 sets, namely user's attributes (age, function, title, department, etc.), attributes of the resource or object (smart meter database, IED control console, users' measurement data, etc.), action attributes (reading, writing, approval, etc.) and environment attributes (time, location, IP, etc.). Differently from the RBAC model, ABAC can support dynamic attributes, however, the administration of users' permissions is more complex [9][14][15-17].

- Role-Centric Attribute-Based Access Control (RABAC)

The Role-Centric Attribute-Based Access Control (RABAC) model was created from the need to add to the RBAC model the advantages of attribute-based models; in this sense one could say that RABAC is an extension of the RBAC model that adds the concept "attributes" and "Permission Filtering Policy (PFP)" to control the permissions that users or objects have on the system[18].

According to the work done by [18], attributes are defined as a set of characteristics of a user or object associated with their environment, for example:

- for a user some attributes would be: Department where he works, title and specialization, work schedule, among others.
- for an object some attributes would be: Serial Number, Model, Location, among others.

In the RABAC model each attribute can be valued, allowing a user or object to have a multi-attribute attribute, for example, a user that has the department attribute can belong to several departments.

The PFP sets the permissions limitations based on user and object attributes, and provides a set of permissions associated with the roles enabled in a given communications session. These permissions are additionally limited by policy filtering.

2.6.Schemes of Cipherring

An adequate encryption scheme is required as part of an authentication protocol to provide security in communications, in this sense, the following are described the schemas used in this work for the creation of the proposed protocols:

- Identity-Based Signcryption (IBSC)

Is a scheme of cipherring proposed by [19] and based on Identity-Based Signcryption (IBSC). Each user generates a pair of keys (public and private) and sends the public key with the confidential information to the trustful entity through a secure channel. The entity returns a certificate that, together with operations of bilinear pairing, enables the user to sign, cipher and decipher the message. In this study, the CBSC scheme was modified, so that computational performance, simultaneous authentication and security could be improved.

- Elliptic Curve Diffie-Hellman Protocol (ECDH)

It is characterized as the generation of a shared secret between two or more entities that have not had prior contact, use an unsecure communication channel and are anonymous. Let E be an elliptic curve on F_q , and Q is a point on the agreed curve (known publicly) and P the secret they want to share. Alice and Bob secretly choose a random integer K_a and K_b respectively, shortly thereafter, Alice and Bob compute a public key with the following form: $K_a * Q$ and $K_b * Q$ respectively, and interchange the generated public keys. Finally, in order to calculate the shared secret P , Alice and Bob multiply their private keys with the public keys inserted: in the case of Alice, it will do the following calculation $P = K_a * K_b * Q$, in the case of Bob he will perform the following calculation $P = K_b * K_a * Q$. A person who wanted to spy on Alice and Bob would have to determine $P = K_a * K_b * Q$ but without the private keys K_a or K_b could not calculate the secret P [20].

- Bilinear Pairing

The birth of the bilinear pairing in the beginning was created as an attack method to cryptographic schemes based on elliptic curves. only until the year 2000 were published the first researches that used bilinear pairing as a solution to cryptographic problems and not as tool.

Bilinear pairing in cryptography has favored the creation of new and creative cryptographic protocols, such as: identity-based cryptography, short signatures, key agreement schemes, among others [21][22].

In this work, bilinear pairing is used to verify identities. The following is the definition and properties of bilinear pairing [21][22]:

- Definition:

A bilinear pairing is a function that projects two additive elements of group G_1 into one element of group G_2 . Bilinear pairing is written mathematically as follows $(G_1, G_1) \rightarrow G_2$.

The system chooses a number of order p , a set G_1 and an additive group and G_2 a multiplicative group of order p .

Properties:

Bilinear pairing has the following properties:

- i. **Bilinearity:** For all $R, S, T \in G_1$, $\hat{e}(R + S, T) = \hat{e}(R, T)\hat{e}(S, T)$ and $\hat{e}(R, S + T) = \hat{e}(R, S)\hat{e}(R, T)$.
- ii. **Non-degeneracy:** $\hat{e}(P, P) \neq 1$.
- iii. **Computability:** \hat{e} can be efficiently computed.

The pairings also have the following properties

- i. $\hat{e}(S, \infty) = 1$ and $\hat{e}(\infty, S) = 1$.
- ii. $\hat{e}(S, -T) = \hat{e}(-S, T) = \hat{e}(S, T)^{-1}$.
- iii. $\hat{e}(aS, bT) = \hat{e}(S, T)^{ab}$ for all $a, b \in Z$.
- iv. $\hat{e}(S, T) = \hat{e}(T, S)$.
- v. If $\hat{e}(S, R) = 1$ for all $R \in G_1$, then $S = \infty$.

2.7. Smart Grid Architecture

2.7.1. Architecture of Smart Grid

The following describes the terminologies and the general architecture of the SG and V2G networks used as the basis for the creation of the proposed protocols. The general figure of the architecture is shown in figure 2.4.

- **Supervisory Control and Data Acquisition (SCADA):**
A system that captures information from several sources of production and consumption of energy for generating indicators that enable the making of decisions automated and controlled in the electrical system.
- **Intelligent Electronic Device (IED)**
Any equipment controlled by a microprocessor connected to the electrical wire for interacting and administering it, e.g., equipment for the monitoring, control or protection of circuits, distribution or dissemination of electrical energy, etc.
- **Outdoor Field Equipment (OFEs)**
Equipment of the SG network located on streets, as converters, gateways, etc.
- **Smart Meter (SM)**

These are devices that have sensors to measure and send information about the electricity consumed to the power company. It also has the ability to receive information with instructions.

- **Aggregator (LAG)**

SMs and EVs cannot directly send information to the operator, they send information to aggregator that has the task of grouping information from several devices, in order to decrease the cost in communications.

- **Cloud Service Provider (CSP)**

It is an entity that provides cloud computing services based on its existing platforms and applies certain rules and fees for these services.

- **Electric Vehicle (EV)**

Term “electric vehicle” can be attributed to cars, motorcycles, boats, planes and other vehicles powered by electric energy stored in batteries.

- **Charge/Discharge Stations (CDS)**

Stations that are part of the V2H architecture and charge or discharge the energy of the electric vehicles’ batteries.

- **Authentication Server (AS)**

An authentication server validates the identity and credentials of EVs and stores their corresponding attributes. A distributed architecture with a Central Authentication Server (CAS) located in a control center and connected to several Substation Authentication Server (SAS) can be used for a large system, as the SG network.

- **Control Center (CC)**

It is an operations center that controls all the electric network.

- The energy providers have employees who want different types of work on SG. such as: vendors engineers (VE), maintenance personnel (MP) and security officer (SO).

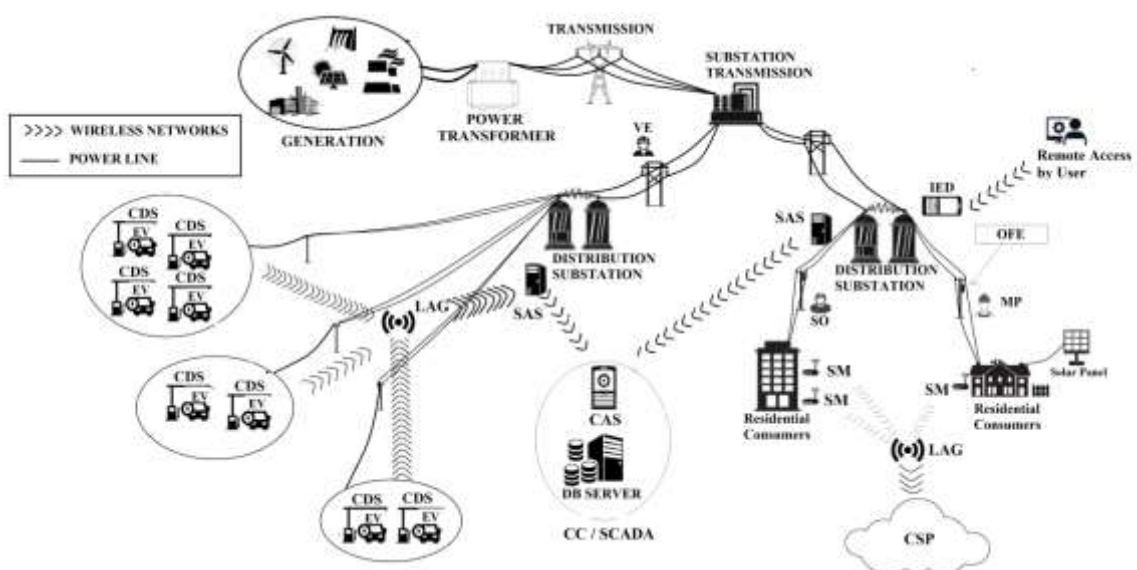


Figure 2.4- Smart Grid Architecture

2.7.2. Smart Grid Communications Architecture

One of the most critical elements of the SG network is the communications layer. Communication networks can be represented in a multilayer architecture. The classification is given by the data rate and scope of coverage. This architecture is composed by Kuzlu et al. [24]:

- Customer premises area network, i.e., Home Area Network (HAN)/Building Area Network (BAN)/Industrial Area Network (IAN):

Among the services that can be offered from the HAN, BAN and IAN (figure 2.5) networks are the automation of relays and buildings by sending and receiving electrical measurement data between the devices and a controller installed in the customer's home, building or industry. the HAN, BAN and IAN networks. The communication requirements to be met by the applications are: low energy consumption and cost, simplicity and secure communication. Therefore the communication network must support a data rate of over 10kbps and a coverage radius of up to 100 m. The widely used technologies to support the services are: ZigBee, WiFi, Z-Wave, PLC, Bluetooth and Ethernet[24].

- Neighborhood Area Networks (NAN)/Field Area Network (FAN).

Services supported by NAN and FAN networks (figure 2.5), such as Advanced Metering Infrastructure (AMI) and Vehicle to Grid (V2G), among others, need to transmit and receive data from many clients to a data hub or substation. Therefore the communication network must support a data rate of between 100kbps to 10 Mbps and a coverage radius of up to 10km. The services of the NAN or FAN networks can be supported through ZigBee mesh networks, Wifi mesh networks, WiMAX, PLC, Cellular, Coaxial Cable or Digital Subscriber Line (DSL) [24].

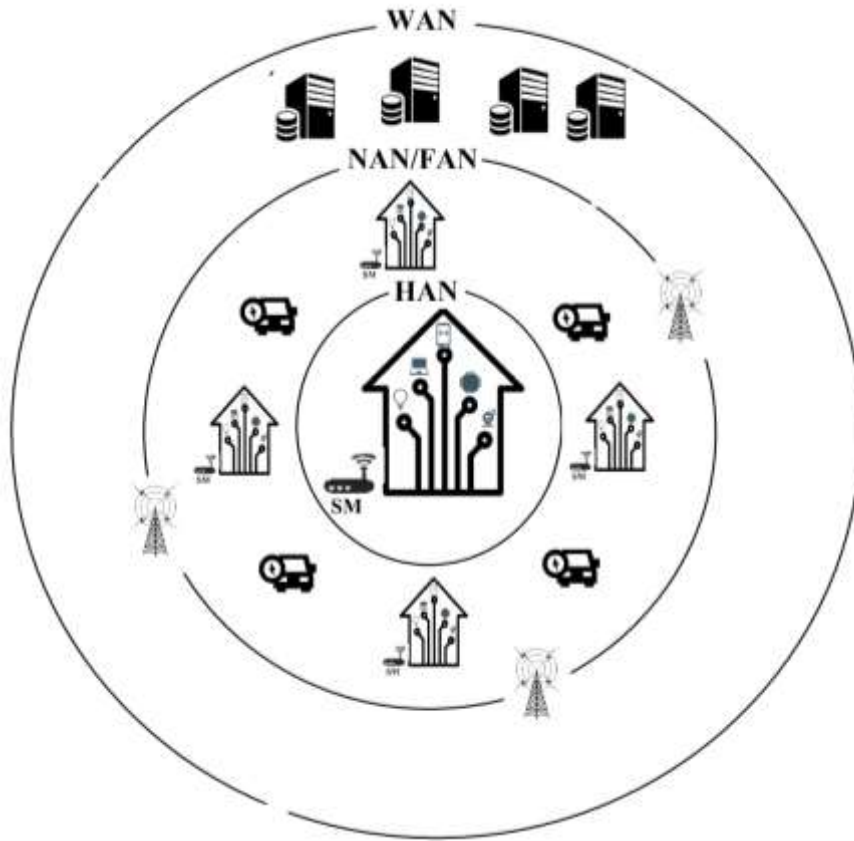


Figure 2.5- Segments of the smart grid

Descriptions of the services that are supported by NAN / FAN are discussed below:

- Advanced Metering Infrastructure (AMI)
In the traditional systems of public services (electric, gas, water) the service providers performed a periodic consumption measurement to carry out the billing process and demand analysis. With Advanced Metering Infrastructure (AMI), power providers can perform bidirectional communications in real time between the SM and a centralized control center. This infrastructure is responsible for measuring, retrieving and analyzing energy consumption data obtained from smart contacts and sent by control commands. [19-20].
- Vehicle to Grid (V2G)
Applications involving electric transport such as V2G are considered to be powerful approaches to creating services based on renewable energy. The V2G allows Electric Vehicles (EVs) to become valuable resources for the SG, because it can interact with the electrical network in different ways (supplier, store, consumer), allowing a better management of energy in the entire electrical network [24] [26].
- Wide Area Network (WAN)

For services supported by WAN networks (figure 2.5), such as control, monitoring and wide-area protection, they require the transmission of a large number of data points in real time to control the stability of the power system. For WAN networks, communications technologies are required to work with a data rate between 10Mbps and 1Gbps and a coverage of up to 100

km. WAN communications can support technologies such as optical fiber, cellular networks, WiMAX and satellite communications [24].

2.8.AVISPA Tools

Automated Validation of Internet Security Protocols and Applications, known as “AVISPA Tools”, was a project developed by several institutions of the European Union that aimed to develop a technology and tools capable of analyzing the security of the protocols and applications that will be applied in information technologies [27].

AVISPA uses its own language to model the protocols called "The High Level Protocol Specification Language (HLPSL)". In the HLPSL language it is possible to model the actions and messages exchanged between the agents during the execution of the protocols.

For the analysis of security of the protocols AVISPA has four modules called Back-Ends with different techniques of automatic analysis of threats against attacks. Only two Back-Ends, the On-the-fly-Model-Checker (OFMC) and the Constraint-Logic-based Attack Searcher (CL-AtSe) will be used, since they are the only ones that support the operations used in the protocol proposed [27,28].

The results of the security analysis of the AVISPA tools show the word "SAFE" on the screen, if there are no security problems in the protocol, along with statistics of the back-end performance performed, and the word "UNSAFE" is accompanied by a report of the security problems found and the executed attack[28].

In the case of back-ends used in this dissertation, the statistics describe the following:

- For the OFMC Back-end :
 - **ParseTime**: describes the time in seconds that the system takes to analyze the protocol.
 - **SearchTime**: Write the time in seconds that I take the system to perform a search for attacks that can affect the system.
 - **VisitedNodes**: describes the visited nodes of the binary tree built by the OFMC backend. The root node of tree represents the initial state of the protocol and the children nodes represent the decisions that the protocol can take at each step. Each node can have infinite child node.
 - **Depth**: describes the depth of research performed within the trees (bearing in mind that trees may have infinite nodes)

- For the CL-AtSe Back-end:
 - **Analysed**: Describes the number of analyzed states of the protocol.
 - **Reachable**: describes the number of reachable states of the protocol, where an attack can be performed.
 - **Translation**: describes the time in seconds that the system takes to translate the HLPSL code to the IF (Intermediate Format)
 - **Computation**: describes the time in seconds that the system takes to analyze the protocol.

The Dolev-Yao intruder model [29-30] is considered, with the following characteristics: cryptography is flawless (unbreakable by the intruder) and messages are exchanged over a network that is under its control; the intruder can intercept messages and analyze them if he possesses the corresponding keys for decryption; thus he/she acts as an omnipresent agent which cannot make cryptanalysis.

2.9.References

- [1] National Institute of Standards and Technology. “An Introduction to Computer Security: The NIST Handbook”. Special Publication 800-12. out 1995.
- [2] Rendell, R. “Talking to Strange Men, FIPS PUB 180-3, Secure Hash Standard (SHS)”, NIST, Hutchinson, 1987.
- [3] Stallings, William. “Cryptography and network security: principles and practice”. sixth ed. Boston: Pearson, 2014.
- [4] International Telecommunication Union, The International Telegraph And Telephone Consultative Committee “Recommendation X.800”, 1991
- [5] Shirley, “R: Internet Security Glossary, Version 2 RFC 4949; Internet Engineering Task Force”, 2007.
- [6] S.M. Furnell, P.S. Dowland, H.M. Illingworth, P.L. Reynolds, “Authentication and Supervision- A Survey of User Attitudes” *Computers & Security*, vol. 19, pp. 529-539, 2000.
- [7] S. Kiljan, K. Simoens, D. Cock, M. V. Eekelen, H. Vranken, “A Survey of Authentication and Communications Security in Online Banking”, *Journal ACM Computing Surveys*, vol. 49, No. 9, 2017.
- [8] G. M. J. Pluimakers and J. van Leeuwen, “Authentication: A Concise Survey”, *Computer & Security*, vol. 5, pp. 243-250, 1986.
- [9] Coyne, E., Weil, T., (2013) "ABAC and RBAC - Scalable, Flexible, and Auditable Access Management", *IT Professional*, vol.15, Issue 3.
- [10] D. Rosic, U. Novak, and S. Vukmirovic, “Role-based access control model supporting regional division in smart grid system,” in *Proc. 5th Int. Conf. Computational Intelligence, Communication Systems and Networks*, Jun. 2013, pp. 197–201.
- [11] H. Cheung, A. Hamlyn, T. Mander, C. Yang, and R. Cheung, “Role based model security access control for smart power-grids computer networks,” in *Proc. Power Energy Soc. Gen. Meet.—Convers. Del. Elect. Energy 21st Century*, 2008.
- [12] H. Cheung, A. Hamlyn, T. Mander , “Strategy and role based model of security access control for smart grids computer networks,” in *Proc. 2007 IEEE Canada Electric Power Conference (EPC 2007)*, Montreal, Canada, Oct. 2007.
- [13] Y. Zhu, D. Huang, C.-J. Hu, and X. Wang, “From RBAC to ABAC: constructing flexible data access control for cloud storage services,” *IEEE Transactions on Services Computing*, vol. 8, no. 4, pp. 601–616, 2015.
- [14] N. Saxena, B. J. Choi, “State of the Art Authentication, Access Control, and Secure Integration in Smart Grid”, *Energies* ,vol. 8 Issue 10, pp. 11883-11915, 2015.
- [15] M. Joshi, S. Mittal, K. P. Joshi, T Finin, “Semantically Rich, Oblivious Access Control Using ABAC for Secure Cloud Storage”, *Edge Computing (EDGE)*, 2017.
- [16] Y. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer*, no. 2, pp. 85-88, 2015.

- [17] Z. Xu and S. D. Stoller, “Mining attribute-based access control policies from RBAC policies,” in Proc. 10th Int. Conf. Expo Emerg. Technol. Smarter World, Oct. 2013.
- [18] X. Jin, R. Sandhu, R. Krishnan, “RABAC : Role-Centric Attribute-Based Access Control”, Computer Network Security, vol. 7531, pp. 84-96, 2012.
- [19] Li, F., Xin, X. e Hu, Y. (2008) “Efficient Certificate – Based Singryption Scheme From Bilinear Pairings”, International Jurnal of Computers and Applications, v.30, No 2, 2008.
- [20] N. Koblitz, A. Menezes, and S. Vanstone, “The state of elliptic curve cryptography”, Designs, Codes and Cryptography, 19(2-3): pp. 173-193, 2000.
- [21] L. Martinez, “Diseño e implementación eficiente del emparejamiento ê en dispositivos móviles y arquitecturas multinúcleo”, Masters dissertation, Centro de Investigación y de Estudios Avanzados Del I.P.N.,2008
- [22] Menezes, Alfred. (2005) “An Introduction to Pairing-Based Cryptography”, Recent Trends in Cryptography, v. 477, p. 47-65.
- [23] Z. A. Baig, A. R. Amoudi, (2013) “An Analysis of Smart Grid Attacks and Countermeasures”, Journal of Communications, v. 8, No. 8.
- [24] M. Kuzlu, M. Pipattanasomporn, S. Rahman, “Communication network requirements for major smart grid applications in HAN, NAN and WAN”, Computer Networks, vol. 67, pp. 74-88, 2014.
- [25] M. Delavar, S. Mirzakuchaki, M. H. Ameri, J. Mohajeri2, “PUF-based solutions for secure communications in Advanced Metering Infrastructure (AMI)”, International Journal of Communication Systems, vol. 30, 2016.
- [26] M. Tao, K. Ota, M. Dong, “Foud: Integrating Fog and Cloud for 5G-Enabled V2G Networks”, IEEE Network, vol. 31, pp. 8-13, pp. 1099 – 1131, 2017.
- [27] The AVISPA Project: European Union in the Future and Emerging Technologies (FET Open). Retrieved Nov 26, 2016, from <http://www.avispa-project.org>.
- [28] AVISPA Team, “AVISPA v1.0 User Manual”, Project funded by the European Community under the Information Society Technologies Programme, vol. 1, 2006, from <http://www.avispa-project.org>.
- [29] M. Avalle, A. Pironi, R. Sisto, “Formal Verification of Security Protocol Implementations: A Survey”, Formal Aspects of Computing, vol. 26, pp. 99-123, 2014.
- [30] J. López, R. Monroy, “Formal Support to Security Protocol Development: A Survey”, Computacion y Sistemas, vol. 12, pp. 89–108, 2008.

Chapter 3

Authentication and RABAC-Based Access Control Protocol for Smart Grids

Abstract: *Smart Grid requires the guarantee of integrity, accessibility and confidentiality of data. This chapter introduces a protocol of users' authentication and authorization that mitigates internal and external threats. The authentication is based on a cryptographic scheme that uses digital signatures to encrypt data and the authorization is based on roles and attributes of users. Security and performance analyses revealed the protocol is more efficient, in most cases, in comparison to some other protocols, regarding security properties and computational and communication costs.*

3.1. Introduction

Smart Grid (SG) constitutes an aggregation of technologies and subsystems that can be used for the integration of advanced systems of both energy and communication networks and technologies. The use of SG-based solutions enables electrical networks to work in a more efficient, productive, sustainable and transparent way. However, information security is one of the possible problems caused by threats and attacks that affect confidentiality, integrity, accessibility, protection and privacy of data.

Integrity, availability and confidentiality of information either stored or in transit resulting from attacks to SG network security can be jeopardized, change data without permission, cause latency in the network and expose information to clients.

The permissions of a user on the data or devices of the system should be granted only after a process of authentication and authorization of their identity. These privileges can change depending on the role that develops in the system and taking into account the time, space and context of the user.

A broad view of requirements of authentication and authorization in the SG network must take into account the several types of users, as employees (EMP), vendors engineers (VE), maintenance personnel (MP) and security office (SO). Therefore, each user can access some possible uses of the system, as reading, reading-writing, writing and addition-deletion.

In such a context, the authentication and authorization of users in the SG network are challenging, once devices and other resources can be accessed both locally and remotely through the Internet, and the access to resources must be treated specifically for the functional demands of each user. Therefore, only authenticated users should perform actions duly authorized for the devices (assigned according to each user's roles and attributes) and other resources in a controlled and scalable way.

One of the access control models that makes use of roles (RBAC) and attributes of the user or objects is the Role-Centric Attribute-Based Access Control (RABAC) model. In the RABAC model attributes are defined as the characteristics of the users or objects associated with their environment (company name, work department, academic titles, years of experience, among others); filtering policies are implemented, in order to limit actions that may perform users or objects on the system.

This chapter introduces a protocol for mutual authentication and authorization between the user and an SG network authentication server. The protocol is partially based on protocols proposed by Saxena et al. [7] and Vaidya et al. [9] and enables a dynamic authorization for each user's role through bilinear pairing and some concepts and techniques of the Certificate-Based Signcryption (CBS) [3].

After authentication, an authorization can be provided and maintained for some limited time, so that each user can undertake only the authorized actions by controlled access and its respective validity. The protocol is based on the authentication of the following two factors: identification verification and a One-Time Password (OTP) sent through a terminal cellular to the user accessing the device. OTP also enables the user to check the sender's validity. A session key is shared between the device and the user through a certificate-based encryption.

The chapter is organized as follows: Section 2 presents some related works; Section 3 addresses some studies on user's authentication and authorization in the SG network; Section 4 introduces the proposed protocol; Section 5 reports a performance analysis of the protocol and the meeting of security properties is characterized; Section 6 provides the results of the formal verification of the protocol; finally, Section 6 is devoted to the conclusions and suggests some future studies.

3.2. Related Work

Studies on security solutions to attacks performed by users (operators, maintenance personnel, supplying engineers, and security employees) have been considered. This chapter focuses on studies related to protocols designed for the control of access to resources and devices and authorization of each user's activities.

Vaidya et al. [9] proposed a centralized server called SSC (Substation Controller) that authenticates users, assigns attribute certificates to users, and keeps access records. According to the author, some important challenges of the SCADA system involve restrictions of computational resources and storage of field devices, low-tax data transmission and necessity of low-latency responses of devices in the entire network. The protocol uses a public key cryptographic system (PKC) based on elliptic curve or ECC (Elliptic Curve Cryptography), and employs a protocol of zero-knowledge proof whose verification is assisted by a server or SAV (Server Aided Verification) and has an AC (Attribute Certificate) [9] for the authorization of services.

Saxena et al. [7] designed a protocol of mutual authentication between the user and the server and an authorization considering the user's role (Role-Based Access Control - RBAC) calculating a hash value based on his/her attributes (Attribute-Based Access Control - ABAC). An architecture of the SG network comprised of IED, SMs, OFEs, and a Central Authentication Server, or ASc, which interconnects the authentication servers of the substations, or ASss, were considered. The authentication of two factors is established. First, authentication is performed through the verification of each user's identity on the substation server. Next, an OTP password is sent to the user's cell phone for checking the identity of the user accessing the device. Finally, a secret key is shared between the user and the device for a safe communication through the bilinear pairing technique.

Cheung et al. [11] developed an access control scheme for SG networks, called Smart-Grid Operation-based Access Control (SOAC) and Lee [2015] proposed the implementation of Role-Based Access Control (RBAC) based on the norm of the International Electrotechnical Commission (IEC) 62351 and using Extensible Access Control Markup Language (XACML).

As in Saxena et al. [7], the use of RBAC was considered in this research for the control of access to components and resources of the SG network and ABAC for the validation of the user's identity for taking advantage and mitigating the disadvantages of each model System Model.

3.3. System Model

Below are some SG network terminologies that treat the architectures used as a basis and favor the understanding of the protocol.

- **SCADA (Supervisory Control and Data Acquisition):**
A system that captures information from several sources of production and consumption of energy for generating indicators that enable the making of decisions automated and controlled in the electrical system.
- **IED (Intelligent Electronic Device)**
Any equipment controlled by a microprocessor connected to the electrical wire for interacting and administering it, e.g., equipment for the monitoring, control or protection of circuits, distribution or dissemination of electrical energy, etc.
- **SM (Smart Meter)**
Equipment whose sensors measure and send information on the consumed energy to the electric company. It can also receive information with instructions.
- **OFEs (Outdoor Field Equipment)**
Equipment of the SG network located on streets, as converters, gateways, etc.
- **AS (Authentication Server)**
A server that validates users' credentials and identifications and stores the attributes and roles that correspond to each of them. A distributed architecture with a central AS (CAS) located in a center of operations is acceptable for a large system, as the SG network, and several AS that might be located in the substation (SAS) can be connected to it.

Figure. 3.1 shows a possible SG network architecture composed of SMs installed in clients' houses, OFEs distributed in different regions of a city, and IEDs located in subsections. Such devices can be accessed by different users (MP, VE, SO both locally and remotely).

On the other hand, the CAS concentrates securely all the information sent by the SAS is installed in a Control Center (CC). Communication in the SG network is supported by the DNP3 or IEC 61850 and WAN / Cellular technologies for wireless communication. ,

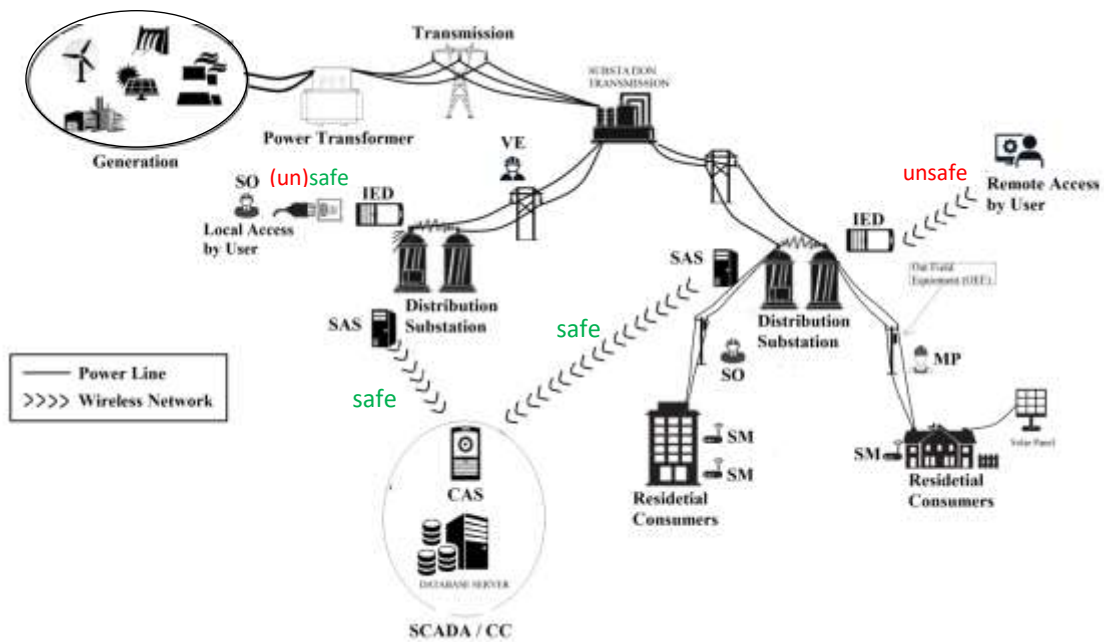


Figure 3.1- Architecture of a Smart Grid System

3.4. Adversary Model

We consider the architecture shown in figure 3.1, where the communication channels between the SAS and CAS, between the local user and the IED are safe and efficient, as well as the SMS channel through which the token is sent. IEDs are located in secure buildings. On the other hand the communication channels of the remote user and the IED and the channel of communication between IED and SAS are considered to be unsafe.

When an authentication and authorization protocol is run on a communication network, attacks on the system are very likely to occur. The following assumptions about attacks are valid on the SG network considered:

- An attacker can execute a replay attack between the user and a remote device, intercepting the user's messages to forward the message, after a while, to the remote device, causing latency in the system;
- The attacker can also acquire the credentials of an authentic entity of the system and pretend to be it to try to join the network;
- A man-in-the-middle (MiTM) attack can also be performed between the user's communications and the remote device, the attacker can make the authentic participants believe that they are exchanging messages between them, but it is the attacker who is receiving and sending all messages exchanged between the user and the remote device;
- It is also possible that an attacker can intercept, manipulate and change the information of the messages exchanged in the system;
- An authenticated user can alter settings of system security policies to execute unauthorized tasks or access an unauthorized device to obtain confidential information. This same attacker can execute a repudiation attack to hide his actions;
- There are many internal or external actors who can make attacks, but in this work we consider the risks posed by employee (MP, SOP, PO) attacks that can affect the system due to an inappropriate authentication and authorization model.

3.5. Proposed Protocol

This section introduces the protocol proposed for both authentication among devices and a dynamic role for an attribute-based access control, so that security properties can be achieved more efficiently regarding computational and communication costs, in comparison with other protocols that address similar issues. The protocol is partially based on those designed by Saxena et al. [7] and Vaidya et al. [9] and use some concepts and techniques present in Certificate-Based Signcryption (CBS) [4] and Pairing-based cryptography (PBC) [8].

The proposed protocol considers, initially, the case of remote users aiming to be authenticated for accessing an IED; this is the case that involves greatest risks. The case of local users is treated in section 3.5.1, where some alterations in the proposed protocol are presented.

Figure 3.2 shows the general the iteration between the entities considered in the protocol.

1. The protocol starts when the PM user sends a remote management request to an IED device along with data for their authentication,
2. IED sends the received user data to the SAS for validation
3. If SAS does not have a user, it requests help from the CAS to authenticate the user, if CAS does not have the user's information, sends a message to the SAS to disconnecting the communication with that user. On the other hand, if the user is authenticated by SAS or CAS, a message is sent to the IED with the user's permissions (role), data for the generation of session stability values, and a request for the user MP to send a token by SMS.
4. The parameters sent by SAS, the IED device calculates a session key and other values with the parameters sent by SAS, which enable a secure message to be sent with verification data and the session key to the MP user.
5. Finally the user finds and verifies the identity of the IED and the SAS by performing operations with the data received by the IED and the token received by SMS. For the sake of clarification regarding protocol description, the insecure dotted channels will be drawn with dotted lines and the secure channels will be drawn with solid lines.

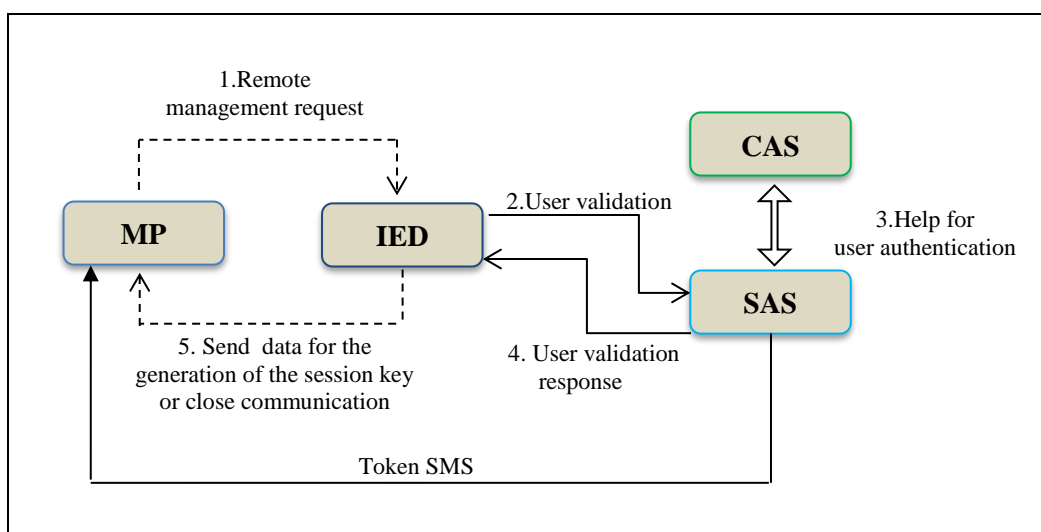


Figure 3.2- General scheme of the proposed protocol

Each user plays a role (according to their functions) assigned by an AS (Authentication Server). The authentication and authorization system is based on CBS with bilinear pairing [7]. Below are the assumptions of the proposal based on the architecture shown in Fig. 3.1.

- In case of a physical access of the devices, a user's interface provides data input/output for each device and performs computational calculations.
- The scenario presented is similar for IEDs, SMs, and OFEs. In this chapter, the protocol is represented with IEDs, however, it can be easily extended to other types of devices.
- Each user registers their data (public key, identity, role, telephone, etc...) on site in the corresponding substation.
- The communication channel between a device and an SAS is secure.
- The clock of the devices is assumed to be synchronized with the clock of the system.

Figure 3.3 shows the proposal that comprises three phases, namely 1) system initialization, 2) user and device registration, and 3) access control of device users

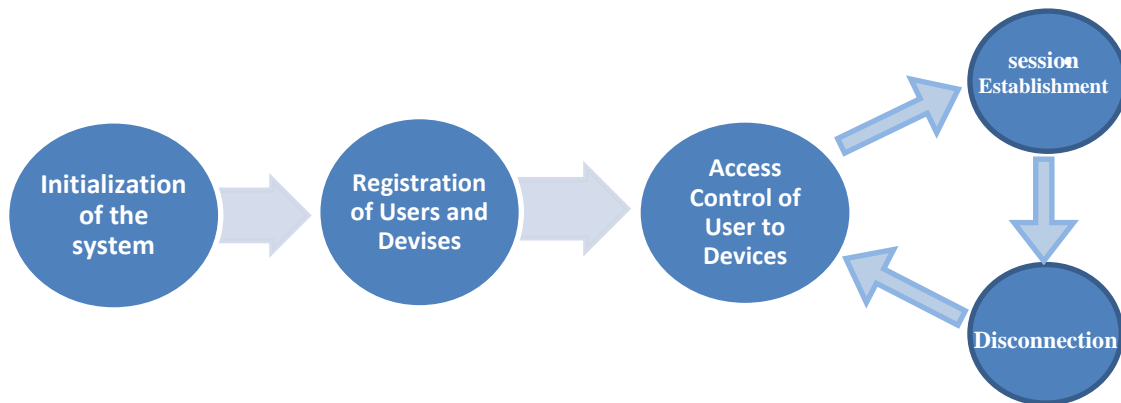


Figure 3.3 Phases of proposed protocol

Table 3.1 shows the symbols and their lengths in bits used in this study.

Table 3.1- Symbols and Cost in bits (Saxena et al. [7]).

Symbol	Description	Length (bits)
Name	User's name	128
ID	User's identification	128
$H()$	Hash function	64
x	Private key	128
y	Public key	128
k	Session key	128
role	User's role	64
L	Localization of the user	32
T	Token	3
t	Timestamp	64
*	Multiplication Operator	-
\hat{e}	Bilinear pairing	-
SAS	Authentication Server of the Substation	-
CAS	Authentication Server of the Control Center	-
Cert	Digital Certificate	128
P	Point of the Elliptic curve	128
\oplus	XOR Operator	-

1st Phase: Initialization of the system:

Two elliptic groups G and G_T of q and P order, as well as a group G -generating element are chosen. G and G_T are supposed to be related to a non-degenerative pairing and a bilinear map that can efficiently compute [6]:

$\hat{e} : G \times G \rightarrow G_T$, such that $\hat{e}(P, P) \neq 1_{G_T}$ and $\hat{e}(aP_1, bQ_1) = \hat{e}(bP_1, aQ_1) = \hat{e}(P_1, Q_1)^{ab} \in G_T$ for all $a, b \in Z_q^*$ and all $P_1, Q_1 \in G$. The hash functions of the system are defined: $H_1: \{0,1\}^* \rightarrow G$, $H_2: \{0,1\}^* \rightarrow Z_q^*$ and $H_3: G_1 \rightarrow Z_q^*$.

Finally, the CAS and all servers of the substations (SAS) define an elliptic curve on a finite field $E(\mathbb{F}_q)$ and parameters $\{G, G_T, \hat{e}, P, H_1, H_2, H_3\}$ are published.

According to the public parameters, the SAS of the substations choose a private key $x_{sas} \in Z_q^*$ and calculate their public key $y_{sas} = x_{sas} * P$ to be published in the substation identity (IDsas).

2nd. Phase: Registration of Users and Devices

- a) All users and devices must register on-site in the assigned substation. The registration of a user starts when he/she chooses an ID_u identity and an $x_u \in Z_q^*$ private key and calculates a public key $y_u = x_u * P$. The user sends to SAS a message containing both public key and identity $\{y_u, ID_u\}$. SAS saves the data received y_u and ID_u , calculates $P_u = H_1(ID_u, y_u, role, celular\ number, No.\ Identity)$ and $Cert_u = P_u * x_{sas}$,

associate the user's attributes, as name, telephone number, dependence and role and sends a message with the data hash associated with the user $\{P_u\}$. In the figure 3.4 shows a summary of the registration phase of the user,

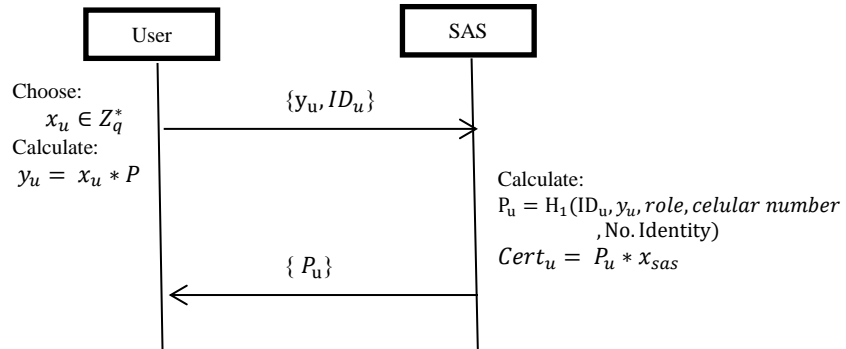


Figure 3.4- User's registration phase

- b) For the registration of a device that makes part of a substation, an identity (ID_{ied}) of the device is chosen; a random number $x_{ied} \in Z_q^*$ is chosen, to be used as its private key, and to calculate a public key $y_{ied} = x_{ied} * P$; then, the IED sends to SAS a message $\{y_{ied}, ID_{ied}\}$ containing a public key and the device identity. SAS keeps the data received y_{ied} and ID_{ied} , calculates $P_{ied} = H_1(y_{ied}, ID_{ied}, L, serial)$ and $Cert_{ied} = x_{sas} * P_{ied}$ and sends IEDi a $\{Cert_{ied}\}$ message to be kept in the device. $Cert_{ied}$ certificate is published in the network. The following shows in figure 3.5 a summary of the registration phase of the devices IEDi,

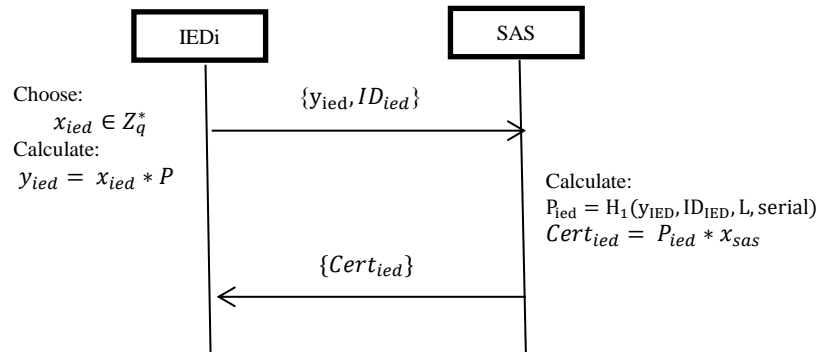


Figure 3.5- Device registration phase

3rd. Phase: Authentication Server of the Substation

The access control phase of the device consists of the following steps:

- 1) ----->

This phase starts when the user sends IEDi a $\{P_u, y_{ied}, L, t_1, H_{m1}\}$ message, where L is the user's location, t_1 is a timestamp of the creation of the message and H_{m1} is a hash of the message that guarantees integrity.

$$2) \quad \xrightarrow{\text{IED } \{P_u, y_{IED}, L, t_2, H_{m2}\} \text{ SAS}}$$

When IED_i receives the message, it calculates an $H'_{m1} = H_1(P'_u, y'_{IED}, L', t'_1)$ hash with the values received and compares $H_{m1} = ? H'_{m1}$. If the values are different from IED_i , the connection is interrupted; otherwise, message $\{P_u, y_{ied}, L, t_3, H_{m2}\}$ is forwarded to SAS, where t_2 is a new timestamp value and hash of message $H_{m2} = H_1(P_u, y_{ied}, L, t_3,)$.

SAS calculates the certificate $Cert_u = P_u * x_{SAS}$ and searches of the user's data that match the certificate. If the certificate does not correspond to any user, the SAS sends the $\{P_u\}$ message to CAS for searching the user's identity and authorizations in the system-wide registry.

If CAS does not find the user's identity, or has no authorizations over the device, it sends SAS a message informing on the closing of the connection. On the other hand, if the above-mentioned information is found, CAS sends SAS a message containing the user's certification and the role assigned $\{Cert_{ied}, role\}$.

SAS checks if the user has an active session in the system. If so, SAS compares the data of the localization of the message received with the localization of active session $L = ? L'$. If they are different, the connection is closed; otherwise, SAS chooses a token T , calculates $H_{m3} = H_1(Cert_u, role, T, t_3)$ and sends the $\{Cert_u, role, T, t_3, H_{m3}\}$ message to IED_i , where t_3 is the new timestamp of the message. Simultaneously, they send token T to the user's telephone number registered through a text message (SMS).

$$3) \quad \xleftarrow{\text{IED } \{Cert_u, role, T, t_3, H_{m3}\} \text{ SAS}}$$

IED_i receives the message, computes the received message hash H'_{m3} and compares $H_{m3} = H'_{m3}$. If they are different the IED closes the connection, otherwise, it chooses $r \in Z_q^*$ and calculates $X_1 = r * H_2(Cert_u + Cert_{ied})$; $w_1 = X_1 \oplus (x_{ied} * y_u)$. It randomly chooses a sufficiently large session key $K_s \in Z_q^*$ and calculates $z = X_1 + w_1$, and $\varphi_k = H_2(w_1 || T) \oplus (z || K_s)$. IED_i sends a $\{\varphi_k, X_1, t_4, H_{m4}\}$ message to the user, where t_4 is a new timestamp and H_{m4} is the hash of message.

$$4) \quad \xleftarrow{U \{ \varphi, X_1, t_4, H_{m4} \} \text{ IED}}$$

The user must calculate the following values for the recovery of the session key that is in the message: $w_1 = X_1 \oplus (y_{ied} * x_u)$ and perform an **xor** operation $\varphi_k \oplus H_2(w_1 || T) = (z || K_s)$, where T is the token sent to the user's telephone number registered through a text message (SMS) and K_s is a symmetric key for communication between the user and the device. Figure 3 shows the messages exchanged, variables calculated and verifications performed in phase two.

After the session key has been calculated, the user performs a SAS identity verification by doing a bilinear pairing $\hat{e}(z, P) = \hat{e}(X_1, P) \hat{e}(y_u, y_{IED})$, which is based on the following sequence:

$$\begin{aligned} (z, P) &= \hat{e}(X_1 + w_1, P) \\ &= \hat{e}(X_1, P) \hat{e}(w_1, P) \\ &= \hat{e}(X_1, P) \hat{e}(y_{IED} * x_u, P) \\ &= \hat{e}(X_1, P) \hat{e}(y_{IED}, P * x_u) \\ &= \hat{e}(X_1, P) \hat{e}(y_{IED}, y_u) \end{aligned}$$

Figure 3.6 shows the messages exchanged, variables calculated and verifications performed in phase two.

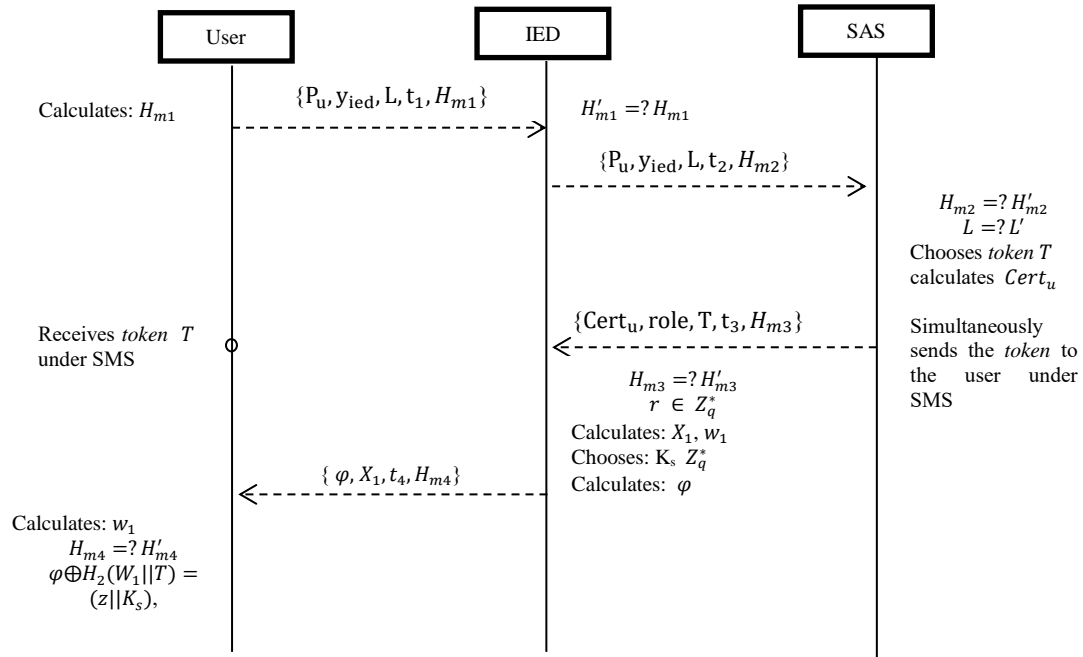


Figure 3.6- Access Control Phase for Remote Users

3.5.1 The Case of Local Users

The proposed protocol was initially designed taking into account the protection of the system in the scenario that has the greatest risks, in this case, the authentication and access control of remote users. Of course, if the proposed protocol ensures secure authentication and access control for remote users, some characteristics for the authentication process could be maintained for local users, with some alterations due to the physical presence of the user near to the IED.

The necessary alterations for treating local users are listed below:

- a) withdrawing the hash H_{m1} from the message 1 which is sent from the User to the IED, and withdrawing the hash H_{m4} from the message 4 that is sent by the IED to the User. Due to the fact that the user is connected with the IED equipment directly in the same place, making it impossible to carry out an attack that can change the integrity of the message.
- b) withdrawing the timestamp t_1 from the message 1 that is sent from the User to the IED, and removing the timestamp t_4 from the message 4 that is sent by the IED to the User. Due to the fact that the user is connected with the IED equipment directly in the same place, making it impossible to perform a message redirection attack.

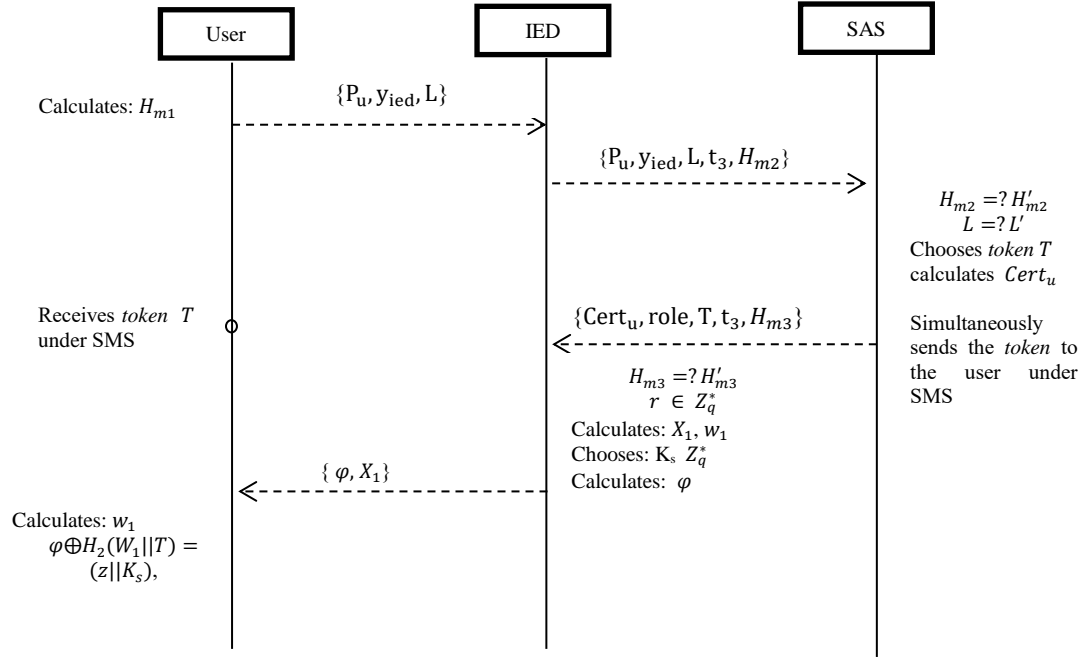


Figure 3.7- Access Control Phase for Local Users

Figure 3.7 presents the Access Control phase for local users. We observed that the number of messages is still the same as the process in remote users; however, the Hash generation, t verification operation and the timestamp of messages 1 and 4 were removed from the protocol.

3.6. Analyses of Security and Performance

This section addresses the analyses of security and performance of the proposed protocol and a comparison with the protocols presented in Vaidya et al. [9] and Saxena et al. [7], as they consider authentication between the user and the server while attempting to access a device of the SG network.

3.6.1. Analysis of Security

This subsection reports on an analysis of authentication, establishment of the session key, preservation of privacy and resistance to different attacks of the proposed protocol.

- 1) **Mutual Authentication:** is established between each User / IED and respective SAS. SAS authenticates the user by checking $Cert_u = x_{SS} * P_u$, each user authenticates the SAS using T token in the session key calculation phase (in which the identity of the substation can also be verified) and in the verification phase using public key y_{IED} the identity of the IED_i is verified.
- 2) **Establishment of the session key:** each session key K_s is randomly generated and shared by IED during each authentication; therefore, it is valid for a user only during a specific session.

- 3) Preservation of Privacy: the user uses the temporary identifier P_u to authenticate, so the user's identity does not need to be changed in the messages and is secured in the authentication server databases.
- 4) Protection to integrity: the protocol protects the integrity through *hash* functions in each message transmitted by the network (H_{m1}, H_{m2}, H_{m3} and H_{m4}). If an adversary intercepts a message and intentionally changes a transmitted parameter, the *hash* value of the message will not coincide in the receiver and the connection will be interrupted.
- 5) Prevention against attacks

The protocol resists to the following attacks:

- Personification: an attacker must know the victim user's identity and secret key. However, he/she cannot obtain parameter $Cert_u$ without the secret key. A session key is generated whenever the user is authenticated in a device for avoiding the use of old parameters in other devices;

- MITM: after receiving a message in the IED device, SAS send an OTP through another channel for verifying the identity and protecting the system from such an attack. Therefore, the user must perform operations with values contained in the message received and OTP sent by the server for obtaining the session key and validating the identity of both device and server;

- Repetition and Injection: an attacker can intercept a message to perform a repetition attack and also inject data. All messages have a similar *timestamp*(t_i) and values randomly chosen for each session, as r, T, K_s and *hash* functions for verifying the integrity of the message and resisting to the attack;

- Redirectioning: whenever a new user tries to access a device, he/she must provide information on localization to the device. If the same user tries a second access, the server checks their localization and compares it with the localization of the first session $L_1 =? L_2$. If the information is different, the server rejects the second connection;

- Attacks by internal personnel: the authentication of clients and maintenance personnel is multifactorial, which contributes to security in case of stealing of credentials. Moreover, users can access only the reading of functions of the role assigned, so that other information cannot be extracted/modified.

- Known Key: the protocol is resistant to such an attack because each session has a different key and the OTP sent to the user is required for its calculation.

- Repudiation: A user can modify the system only after his/her identification and authentication; therefore, a malicious user or invader cannot change the security parameters of the device.

- DoS: The server will allow only the validated user to access the device, once only a validated user can send the right parameter S_u . Moreover, if more than one session is requested, the server checks the location of the requests. If differences among the locations from the same user's requests are detected (the system has an acceptable localization interval), the system rejects communication for avoiding even DDoS attacks.

Table 3.2 shows a summarized comparison of the security properties of the protocol and the above-mentioned related work. Some characteristics are common to all protocols compared, e.g. mutual authentication and agreement of keys, use of session keys, avoidance of repetition attacks through challenges, timestamps and random numbers during authentication, avoidance of Man-in-the-Middle attacks, as the parameters published in the communication channel are

not enough for the generation of valid messages and session keys by an attacker, and contraposition to personification and repudiation attacks.

Table 3.2- Security Analysis of the protocols.

	Vaidya 2013	Saxena 2016	Proposed protocol
Mutual Authentication and Key Agreement	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes
Integrity	No	Yes	Yes
Privacy	Yes	Yes	Yes
Injection Attacks	No	Yes	Yes
Resistance to the Repetition Attack	Yes	Yes	Yes
Attacks by internal personnel	Yes	Yes	Yes
Attack of known key	Yes	Yes	Yes
Resistance to <i>DoS</i> Attack	Yes	Yes	Yes
Resistance to <i>Man-in-the-Middle</i> Attack	Yes	Yes	Yes
Resistance to Redirectioning Attack	No	Yes	Yes
Resistance to Personification Attack	Yes	Yes	Yes
Repudiation Attack	Yes	Yes	Yes

The protocol designed by Vaidya et al. [9] uses neither hash functions to ensure integrity of messages exchanged on the open channel and avoid Injection Attacks, nor timestamps to resist redirection attacks. Therefore, our protocol offers some advantages regarding security in comparison to the protocol designed by Vaidya et al. [9].

3.6.2. Formal Verification of the Proposed Protocol

This section provides the results of the formal verification of the protocol performed by AVISPA.

3.6.2.1. Modelling of the protocol in HLSPL language

The Figure 3.8 shows the modeling of User, IED and AS entities proposed in the protocol. Figure 3.9 displays the HLSPL code describing the exchanged messages and operations performed by the user in the authentication phase of the proposed protocol

```

role role_U(U,IED,AS:agent,P,Xu,Yu,Yss,IDied, Yied,Certied:text,Kcel:symmetric_key,SND,RCV:channel(dy))

played_by U
def=
  local
    State:nat,
    Pu,Hm1,Hm4,T1,G,X1,T4,W1,Z,R,J,V,L:text,
    Token:message,
    Ks:symmetRic_key,
    M,H1,H2:function

  init
    State := 0
  transition
    1. State = 0  $\wedge$  RCV(start)  $\Rightarrow$  State:=1  $\wedge$  SND(Pu'.Yied'.L'.T1'.Hm1')
       $\wedge$  T1' := new()  $\wedge$  R' := M(Xu',Yss')  $\wedge$  Hm1' := H1(Pu'.Yied'.L'.T1')

      4. State=1  $\wedge$  RCV(G'.X1'.T4'.Hm4')  $\Rightarrow$  State':=2  $\wedge$  W1' := xor(M(Xu',Yied'),X1)
       $\wedge$  V' := xor(G'.H2(W1'.Token'))  $\wedge$  G' := Z'.Ks'  $\wedge$  secret(Ks',sec_1,{IED,U})

end role

```

Figure 3.8- User's role in HLSPL

Figure 3.9 shows the code for AS's role in HLSPL which includes the session function, which describes the establishment of a session combining all entities involved in the authentication procedure, and the environment function, which describes the environment where the protocol is run.

```

end role

role session1(U,IED,AS:agent,
  P,IDied,Xss,Yss,IDu,Papei,Xu,Yu,Xied,Certu,Certied,Yied:text,
  Token:message,
  Sechannel,Kcel:symmetric_key,
  SND,RCV:channel(dy))
def=
  composition
    role_U(U,IED,AS,P,Xu,Yu,Yss,IDied, Yied,Certied,Kcel,SND,RCV)
     $\wedge$  role_IED(U,IED,AS,P,IDied,Yied,Xied,Certu,Certied,Yu,Sechannel,SND,RCV)
     $\wedge$  role_AS(U,IED,AS,P,IDied,Xss,Yss,IDu,Yu,Papei,Certu,Yied,Sechannel,Kcel,SND,RCV)
  end role

role environment()
def=
  const
    p,idied,xss,yss,idu,papei,xu,yu,xied,certu,certied,yied:text,
    u,ied,as:agent,
    token:message,
    sec_1,sec_2,sec_3,sec_4:protocol_id,
    snd,rcv : channel (dy),
    kcel,sechannel:symmetric_key

    intruder_knowledge = {}

  composition
    session1(u,ied,as,p,idied,xss,yss,idu,papei,xu,yu,xied,certu,certied,yied,token,sechannel,kcel,snd,rcv)
     $\wedge$  session1(i,ied,as,p,idied,xss,yss,idu,papei,xu,yu,xied,certu,certied,yied,token,sechannel,kcel,snd,rcv)
     $\wedge$  session1(u,i,as,p,idied,xss,yss,idu,papei,xu,yu,xied,certu,certied,yied,token,sechannel,kcel,snd,rcv)
     $\wedge$  session1(u,ied,i,p,idied,xss,yss,idu,papei,xu,yu,xied,certu,certied,yied,token,sechannel,kcel,snd,rcv)
  end role

```

Figure 3.9- Specification of the session role in HLSPL

Finally, Figure 3.10 shows the following four objectives of secrecy are defined:

- secrecy_of sec_1: represents the session key K_s , which can only be known by the user and the IED.
- secrecy_of sec_2: represents the identity of the user (ID_u), which can only be ascertained by the user and SAS.
- secrecy_of sec_3: represents the role of the user, which can only be known by the user, IED and SAS.
- secrecy_of sec_4: represents the OTP, which can only be known by the user, IED and SAS.

```

Goal
  secrecy_of sec_1
  secrecy_of sec_2
  secrecy_of sec_3
  secrecy_of sec_4
end goal

```

Figure 3.10- Security objectives of the protocol in HLSPL

3.6.2.2. Results of the Security Verification

Two simulations using OFMC and CL-AtSe back-ends were performed and the results (Fig. 3.11) showed the protocol is safe.

<pre> % OFMC % Version of 2006/02/13 SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS PROTOCOL /home/span/span/testsuite/results/artigo_1_v5.if GOAL as_specified BACKEND OFMC COMMENTS STATISTICS parseTime: 0.00s searchTime: 0.55s visitedNodes: 189 nodes depth: 6 plies </pre> <p>a) OFMC back-end</p>	<pre> SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS TYPED_MODEL PROTOCOL /home/span/span/testsuite/results/artigo_1_v5.if GOAL As Specified BACKEND CL-AtSe STATISTICS Analysed : 15 states Reachable : 15 states Translation: 0.04 seconds Computation: 0.00 seconds </pre> <p>b) CL-AtSe back-end</p>
--	---

Figura 3.11- Results of Avispa Security Simulation

Figure 3.11.a) shows the simulation results of the proposed protocol, based on HLPSL code and applying the OFMC backend. In the summary it indicates that the protocol is safe and in the statistics part, it can be seen that the search time was 0.55 seconds, the number of visited nodes was 189 and the depth was 6.

Figure 3.11.b) shows the results of the simulation of the HLPSL code of the proposed protocol, applying the CL-AtSe backend. In the summary part it is indicated that the proposed protocol is secure. In statistics you can see that 15 states were analyzed and 15 states were reached, the translation took 0.04 seconds and the calculation was approximately 0.00 seconds.

3.6.3. Intruder simulation with SPAN

The Security Protocol Animator for AVISPA (SPAN) performs Interactive Message Graphs and variables exchanged between agents of the verified protocols from an HLPSL specification. The SPAN has three modes of simulation: protocol simulation, simulation of an intruder in the protocol and simulation of detected attacks (only for OFMD and CL-ATSE backends) [13].

In Figure 3.12 the simulation of an intruder between the user and the IED is shown, using SPAN:

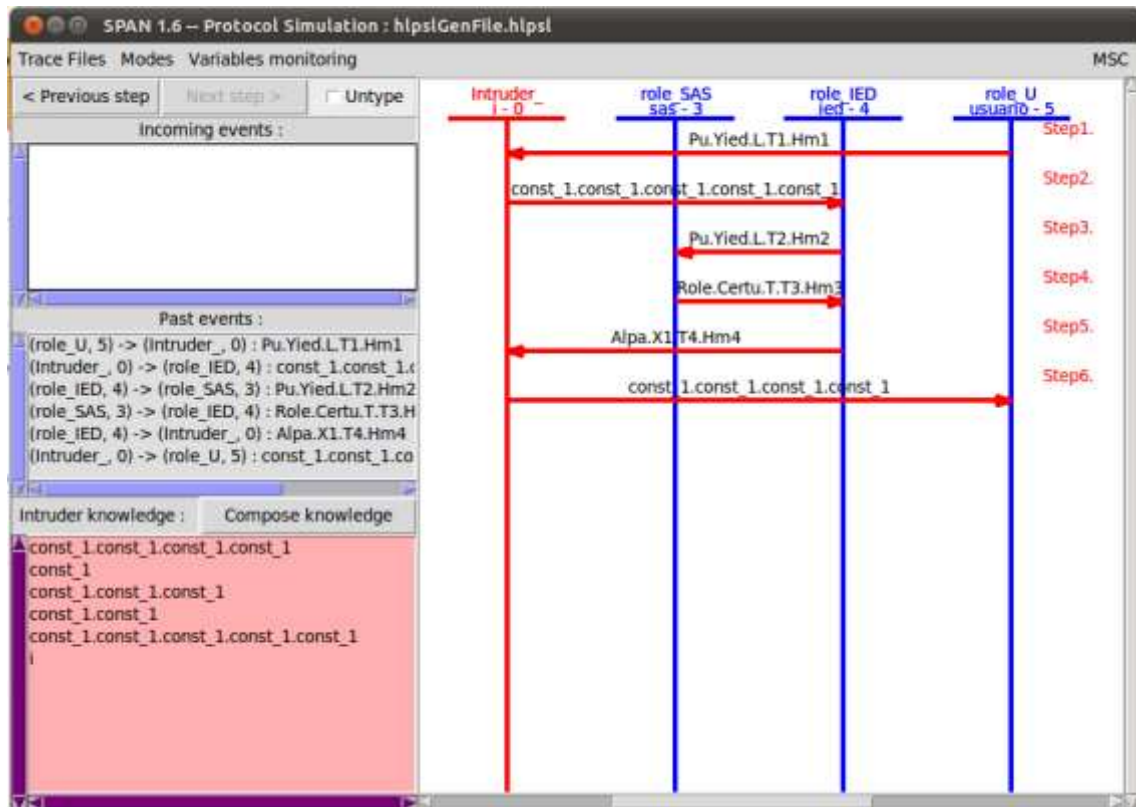


Figura 3.12- Intruder simulation with SPAN

From the simulation with SPAN it is possible to analyze the behavior of the proposed protocol considering the following attacks:

i. Personification Attack:

In this attack an attacker may attempt to pass a valid user. In the SPAN simulation it can be analyzed that there are two scenarios where a personification attack can be executed:

Scenario 1: An attacker can change the Pu, but when the Hash of the message is checked, the IED will find that the message has changed and the connection is terminated.

Scenario 2: An attacker can change the P_u and Hash of the message, this message sent by the attacker when it arrives at the SAS, it will perform an operation with its private key and look for the corresponding user data, but taking into account that the attacker can not generate a true temporary identity the authentication request will be rejected.

ii. MITM Attack:

An attacker can intercept messages between the user and the IED to subtract information to gain access to the system. In the SPAN simulation an attacker establishes a communication with the User and another with the IED. The MiTM attack can be performed in two scenarios:

Scenario 1: The attacker tries to send information to the session key generation: to generate the session key it is necessary to have the user private keys and the IED private key, in addition to the OTP that is sent through a secure channel. Therefore, a possible generate the secret key.

Scenario 2: The attacker attempts to extract information from the message: An attacker may attempt to extract some information from message-4, but cannot decipher the message because it cannot generate the values to do the right operations.

3.6.4. Analysis of Performance

This subsection reports an analytical validation of the protocol's performance, regarding both communication and computational costs. A comparison with other protocols is also provided.

a) Communication Cost

The communication cost is the total number of bits transmitted by the network during the execution of the protocol. The same table of values of [7] shown in Table 1 was used for simplifying the calculations and providing an adequate comparison with the other protocols.

In the sequence below, it is presented the calculation related to the numbers of bits necessary for the messages of the protocol.

Message 1:

$$P_u (128 \text{ bits}) + y_{IED} (128 \text{ bits}) + L (32) + t_1 (64 \text{ bits}) + H_{m1} (64 \text{ bits}) = 416 \text{ bits}$$

Message 2:

$$P_u (128 \text{ bits}) + y_{IED} (128 \text{ bits}) + L (32) + t_2 (64 \text{ bits}) + H_{m2} (64 \text{ bits}) = 416 \text{ bits}$$

Message 3:

$$Cert_u (128 \text{ bits}) + role (64 \text{ bits}) + T (3 \text{ bits}) + t_3 (64 \text{ bits}) + H_{m3} (64 \text{ bits}) = 323 \text{ bits}$$

Message 4:

$$\varphi_k (256 \text{ bits}) + X_1 (128 \text{ bits}) + t_4 (64 \text{ bits}) + H_{m4} (64 \text{ bits}) = 512 \text{ bits}$$

The total communication cost is 1667 bits in the authentication phase if a unique user is considered. Table 3 and figure 4 allow to compare the computational costs between the proposed protocol and the ones proposed by Vaidya et al. [9] and Saxena et al. [7]. In order to have a fairer comparison, and similarly to the procedure adopted by Saxena et al. [7], costs related to the hash and timestamp operations in the messages exchanged in the protocol proposed by Vaidya et al. [9]

According to table 3, the performance of the proposed protocol is higher in comparison to the protocols of Vaidya et al. [9] and Saxena et al. [7], once its number of bits is 317 lower than that of Vaidya et al. [9] and 192 lower than that of Saxena et al. [7].

Table 3.3- Comparison of communication costs

	Vaidya et al.[9]	Saxena et al. [7]	Proposed protocol
Registration Phase	832 bits	-0-	640bits
Message 1	576 bits	704 bits	480 bits
Message 2	448 bits	768 bits	480 bits
Message 3	128 bits	451 bits	387 bits
Message 4	128 bits	704 bits	448 bits
Message 5	320 bits	- 0 -	- 0 -
Message 6	320 bits	- 0 -	- 0 -
Total	2752 bits	2627 bits	2435 bits

In figure 3.13, shows a comparison of the communications costs among the proposed protocol and those of Vaidya et al. [9] and Saxena et al. [7]. The number of users authenticated by the system was considered.

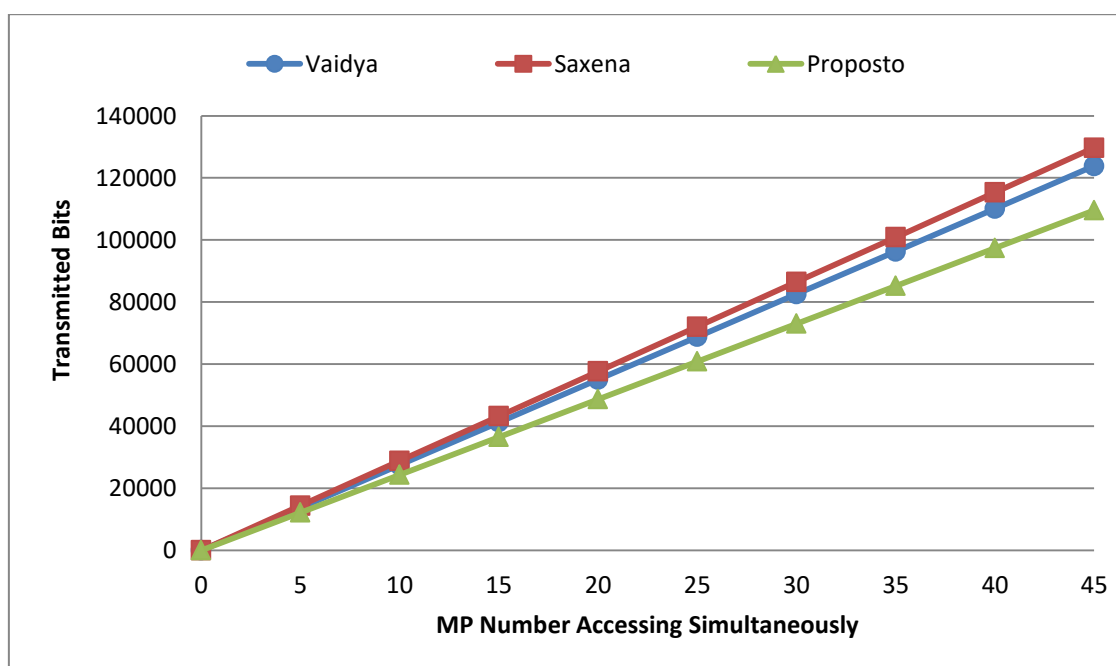


Figure 3.13- Communication Costs of the Protocols

The analysis of communication costs considered remote users; for local users, a reduction of 256 bytes would be obtained due to the withdrawal of timestamping and hashing operations on messages exchanged between the user and the IED. It is possible to verify that the proposed protocol also has superior performance, when compared to others, when a user enters the device locally.

b) Comparison of performance

The abbreviations used in Table 3.4 and the execution times of the operations calculated by Saxena et al. [7] were considered in the comparison of performance.

Table 3.4- Operations and time costs

Operations	Abbreviations	T Execution (ms)*
Hash	H	20
Bilinear pairing	P	197
Addition	A	0,03
Encryption	E	0,23
Decryption	D	0,13
Multiplication	M	17,57

*Source: Saxena et al. [7].

Table 3.14 shows the comparison of the computational costs among the proposed protocol and the other schemas analyzed. Operation **xor** has been omitted, as it is negligible in comparison to the other protocols.

Table 3.5. Comparison of computational costs.

Protocols	ENTITIES			Total
	MP/ UA	IDE/SM/OFE	AS/SSC/TA	
Saxena et al.[7]	4M, 2H, 1D, 1P	6M, 5H, 1A, 1E	4M, 2H, 1A	14M, 9H, 1D, 1P, 2A, 1E
Vaidya et al.[9]	8H, 5A, 4M	4H, 2A, 1M	9H, 5A, 9M	21H, 14A, 12M
Proposed protocol	4M, 4H, 1P, 1A	7M, 3H, 2A	2M, 1H	10M, 9H, 1P, 3A

According to Figure 3.14, the cost of the proposed protocol is lower than those of the protocols designed by Saxena et al. [7] and Vaidya et al. [9], i.e., 68 milliseconds (by an authenticated user) and 111 milliseconds (by an authenticated user) in relation to Saxena et al. [7] and Vaidya et al. [9], respectively.

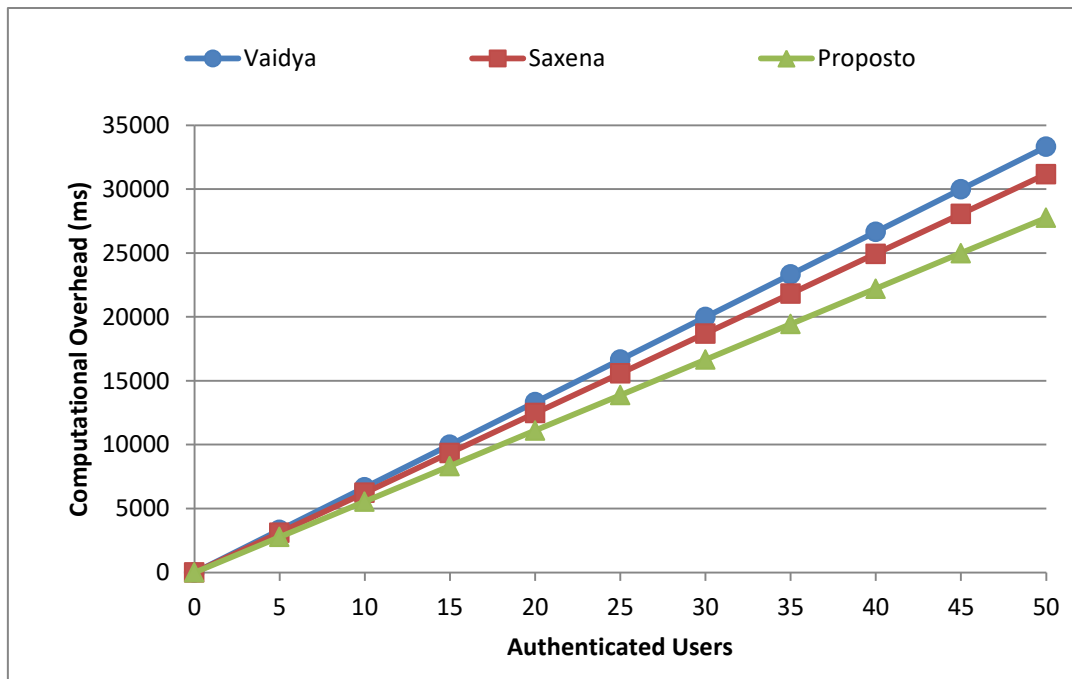


Figure 3.14- Comparison of computational costs between protocols

3.7. Conclusions and Future Work

Research on security in SG networks is fundamental for ensuring privacy of user's data and protection to the electrical infrastructure. One of the security issues that must be adequately addressed is the authentication and authorization of users and devices.

SG control devices must have an appropriate security system for the access control of both remote and local users. Authentication and authorization user's schemes have been developed by the academic community to ensure only users who access the system can perform the authorized tasks.

This chapter introduced a protocol for mutual authentication and authorization between the user and an SG network authentication server. The protocol is partially based on bilinear pairing and some concepts and techniques of Certificate-Based Signcryption (CBS) and performs a dynamic authorization for each user's role.

In comparison with other protocols, it has shown a better meeting of the security properties and its computational and communication cost is lower than that of the protocol designed by Saxena et al. [7] and higher than that of Vaidya et al. [9], which has serious security failures not observed in the proposed protocol.

In summary, the protocol has successfully achieved its objectives. It has provided excellent results regarding security and performance and proven a safe and efficient choice in comparison to other authentication and authorization protocols for SG networks.

AVISPA tool was used to perform a formal verification of the protocol and proved it achieved the security objectives required for successful authentication and authorization.

Future work includes simulation of the protocol in a network simulator, and the development of authentication and authorization protocols for cyber-physical systems (CPS) considering 5G communication models in Smart Grid networks.

3.8. References

- [1] Kamienski, C., Biondi, G., Borelli, f., Heideker, A., Ratusznei, J., Kleinschmidt, J. “Computação Urbana: Tecnologias e Aplicações para Cidades Inteligentes”, XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos – Minicursos, cap 2, p. 51 – 100, 2016.
- [2] Lopes, T., Bornia, T., Farias, V., Fernandes N., and Muchaluat-Saade, D. “Desafios de Segurança e Confiabilidade na Comunicação para Smart Grids”, XXXIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - Minicursos, p. 142 – 186, 2016
- [3] Li, F., Xin, X. e Hu, Y. (2008) “Efficient Certificate – Based Singryption Scheme From Bilinear Pairings”, International Journal of Computers and Applications, v.30, No 2, 2008.
- [4] R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, M. Guizani. “Cognitive Radio Based Hierarchical Communications Infrastructure for Smart Grid,” IEEE Network, vol.25, no.5, pp. 6-14. 2011.
- [5] Coyne, E., Weil, T., “ABAC and RBAC - Scalable, Flexible, and Auditable Access Management”, IT Professional, vol.15, Issue 3. 2013.
- [6] Stallings, W (2014). “Cryptography and Network Security: Principles and Practice”, sixth ed. Boston: Pearson.
- [7] Saxena, N., Choi, B., and Lu, B. “Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid”. IEEE Transactions On Information Forensics And Security. v.11, no.5, 2016.
- [8] Menezes, Alfred. “An Introduction to Pairing-Based Cryptography”, Recent Trends in Cryptography, v. 477, p. 47-65, 2015.
- [9] Vaidya, B., Makrakis, D., and Mouftah, H, “Authentication and Authorization Mechanisms for Substation Automation in Smart Grid Network”. IEEE Network, v.27, P. 5-11, 2013.
- [10] Brown, D., Campagna, M., and Vanstone, S. “Security of ECQV-Certified ECDSA Against Passive Adversaries”. Cryptology ePrint Archive, Report 620, 2009
- [11] Cheung, Herman., Yang, C., and Cheung, Helen. “New Smart-Grid Operation-Based Network Access Control” IEEE Energy Conversion Congress and Exposition P.1203 – 1207, 2015.
- [12] Lee, B., Kim, D., Yang, H., and Jang, H. “Role-Based Access Control for Substation Automation Systems Using XACML”. Journal Information System, V.53, P.237 – 249, 2015.

Chapter 4

Authentication and Authorization Protocol Based on Cloud for Advanced Metering Infrastructure in SG

Abstract: *Electrical networks have evolved rapidly in recent years due to the addition of information technologies, which has given rise to a new concept in Smart Grid (SG). Many elements are considered in the SG network, including the Advanced Measurement Infrastructure (AMI). AMI network collects the energy consumption data of users for the billing and analysis of the energy demand in real time, which requires the protection of the AMI network from any threat that aims at transposing the users' privacy. This chapter proposes a group authentication protocol for key management in an AMI infrastructure integrated with the cloud. The security and performance analysis of the protocol proved its higher computational and communication efficiency in comparison to other protocols.*

4.1. Introduction

The implementation of information technologies in public infrastructures, such as electricity, transportation, aqueducts, among others, has been fundamental for the development of new services and improvements in their efficiency. Electric networks, for example, whose infrastructures were not changed for many years, have benefitted from the new paradigm offered by such technologies regarding generation, transportation and distribution of electricity [1].

The next generation of electrical networks is called Smart Grid (SG). An SG can be considered a Cyber-physical system that mixes systems of physical electricity with a cyber-infrastructure and provides communication with a private network or the Internet [2]. A very important component in SG is the Advanced Measurement Infrastructure (AMI), which integrates advanced sensors, Smart Meters (SM), monitoring systems, and systems of administration of data, and enables bi-directional communication between smart meters and systems of public services. Due to the critical role of AMI in the smart network, it deserves special importance in SG [3].

AMI must not only establish bi-directional communications and process information in real time, but also administer energy, support the connection of millions of devices, administer large amounts of information, architecture in layers (network, communication, electric threads of transmission and generation plants), heterogeneous architecture and security for guaranteeing the integrity, confidentiality and availability of the system [1] [2].

Cloud computation is one of the options that can aid the meeting of AMI requirements, in agreement with the National Institute of Standards and Technology (NIST), which affirms "computation in cloud is a model for enabling convenient, on-demand network access to a shared pool of configurable computation resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal effort or service provider interaction".

The advantages cloud computation offers include services on demand, fast elasticity and pooling of resources and make it a powerful candidate to support applications security and deployment of AMI, because of the reliability, high availability, integrity, scalability and performance it delivers [4].

On the other hand, the integration of AMI with the cloud has some disadvantages, once it must offer a special control, so that only authorized devices can access the different services, and prevent the following security problems:

- Information leakage: data interruption can be caused by human errors or voluntarily by an attacker;
- Data management: due to the high volume of incoming information, efficient filters must be implemented for the management of data and selection, in real time, of those important to be stored and the ones to be discarded;
- Privacy: as it is one of the most important concerns throughout the SG network, a proper authentication and authorization process must be implemented to protect users' privacy.

The implementation of an efficient authentication and distribution key scheme that supports the particular characteristics of the AMI network is fundamental for the protection of data of messages exchanged between different AMI entities through non-secure communication channels. Below are the characteristics of the AMI network:

- AMI is a heterogeneous and complex system, composed of entities with different capacities of computation and communication;
- it provides high availability of services, therefore, the key management scheme must offer mechanisms that protect it against denial of service (DoS) attacks in design;
- the key management protocol must support a number of devices that will grow very fast, once there may be millions of SMs.

Some of the threats that can destabilize the AMI include Denial of Service (DoS), Man in the Middle (MITM), personification and redirection attacks, among others. If such attacks are successful, they can cause a blackout in the cities, altering the customer's billing information or changing the price information sent to clients [3]. Therefore, a protocol that guarantees the confidentiality, integrity and authentication of communication between AMI entities, mainly in integration with the cloud, must be designed.

This chapter proposes a group authentication and key management protocol that considers an AMI architecture integrated to the private cloud. The protocol is based on groups with a binary tree structure for group management and secret keys and uses an anonymous key agreement protocol based on ECDH (Elliptic Curve Diffie-Hellman) for sharing secrets and bilinear pairing for supplying an efficient simultaneous authentication of a group of devices.

The chapter is organized as follows: Section 2 addresses some related works; Section 3 describes the AMI architecture integration to the cloud and reports on an analysis of security requirements; Section 4 introduces the protocol; Section 5 is devoted to an analysis of the security properties; Section 6 describes the formal verification of the protocol; Section 7 focuses on analyses of the performance of the protocol and its comparison with other protocols; finally, Section 8 provides the conclusions and outlines some future work.

4.2. Related Work

The related works addressed are divided into two groups, i.e., one that focuses on proposals for the integration of the cloud and SG and another related to the development of authentication protocols between several entities for the protection against computer attacks and preservation of privacy of the SG network.

4.2.1. Integration of SG and Cloud

Cloud computing represents a new computing paradigm that helps the meeting of requirements of SG networks, as management of millions of devices (smart meters, substations, electric vehicles, among others) in a reliable and scalable system.

This subsection focuses on works on a secure integration of SG networks with the cloud. Genge et al. [4] compared software platforms developed to integrate SG networks with the cloud in a secure way, as parts of projects, such as the D2R (Dynamic Demand Response) project, created to develop an intelligent platform that manages a small SG network. Another project is VS-Cloud, which develops a virtual SCADA architecture for the cloud and aims at a secure control and storage of actions, measurements, incidents or all types of alarms. The authors propose security requirements to the development of secure cloud-based platforms for SG. The projects analyzed in this chapter focus on the confidentiality of system data, not specifically on the authentication of network devices in SG

Bera et al. [2] conducted a bibliographic review of the different applications of cloud computing for the Smart Grid architecture, specifically in 3 areas, namely energy management, information management and security management. Each area includes studies on the overcoming of challenges through the integration of the SG with the cloud, which have given rise to many research opportunities, e.g. authentication and key distribution of an SG network integrated with the cloud.

Ye et al. [5] designed an identity-based security scheme for handling Big Data in SG networks. Actors of the SG network are provided with energy forecast information for the utility company and forecast rate fares for customers. Once user's data can be transported over public networks, more robust measurement protection must be developed. The authors used the cloud to process users' energy consumption information and generate both tariff and power consumption forecasts for further diffusion through a security scheme based on identity and digital signatures.

Saxena et al. [6] proposed an integrated distributed authentication protocol for SG that suggests a mutual authentication among the home environment, power provider, gateways, and AMI. The authors use cloud computing only to create a distributed and hierarchical schema of trusted entities (TA), whose main objective is the quick and easy access to the repository of the public key for the generation of the keys of the devices. Although the scheme is highly secure, it overlooks the advantages of cloud and group authentication.

4.2.2. Key Management and Device Authentication in the AMI Network

A key management scheme must be created for a secure communication and transmission of messages between entities of an AMI network.

This subsection reports on works on the protection of the SG network (or part of it) against computer attacks and preservation of its privacy through authentication and key agreement protocols.

Wan et al. [3] proposed a mixture of symmetric and asymmetric cryptography systems based on elliptic curve and bilinear pairing for the creation of a key management scheme called scalable key management (SKM). The first step is the generation of a session key for a secure point-to-point communication between each SM and the Meter Data Management System (MDMS). Through a tree key creation technique, a Group key that sends messages is broadcasted from MDMS to SM. The scheme does not perform well due to the high computational costs of bilinear pairing operations and high communication costs, once messages must be exchanged between MDMS and each SM for the generation of the session keys.

Nicanfar et al. [7] developed a protocol called SG Key Management (SGKM) that ensures mutual authentication between SMs and the Security and Authentication Server (SAS) in the SG network with the use of passwords and public key infrastructure (PKI). One of the important points is the use of an enhanced version of identity-based encryption (IBC) for a reduction in the key update overhead. The scheme showed the same weaknesses of that designed by Wan et al. [3], i.e., high computational costs due to the use of exponentiation and calculation of a high number of Hash operations. The AMI architectures proposed by the authors are comprised of elements considered passive and trustworthy in an authentication process, i.e., an aggregator (Wan et al. [3]) and a headend (Nicanfar et al. [7]). Therefore, they were not considered in the authors' authentication protocols.

4.3. System Model

Below are the descriptions of the components of the AMI network towards helping the understanding of the proposed architecture and protocol.

- SM (Smart Meter):

A device with sensors that measure and send information on the electricity consumed to the power company and receive information with instructions.

- Aggregator (AG)

SMs cannot directly send information to the operator, therefore, they send it to an aggregator that groups information from several SMs towards decreasing communication costs.

- Cloud Service Provider (CSP)

An entity that provides cloud computing services based on its platforms and applies certain rules and fees for such services. A CSP contains all the management and control servers of an SG network [8], e.g., a head-end system (HES) responsible for 2-way communication with SM that gathers data and sends execution and control commands.

AMI networks must support communications that require services, such as demand response, dynamic electricity pricing, real-time monitoring and measurement. Figure 4.1 shows a possible architecture of the AMI network composed of SMs, AGs and a CSP.

Communications between SM and CSP can be unicast or broadcast. Unicast communications are two-way and usually assigned for the transmission of measurement data, command execution, monitoring, etc. Broadcast communications transmit information containing power tariffs, firmware update packages, etc, from the CSP to the SMs.

This chapter proposes solutions for security in unicast and broadcast communications between CSP and SMs.

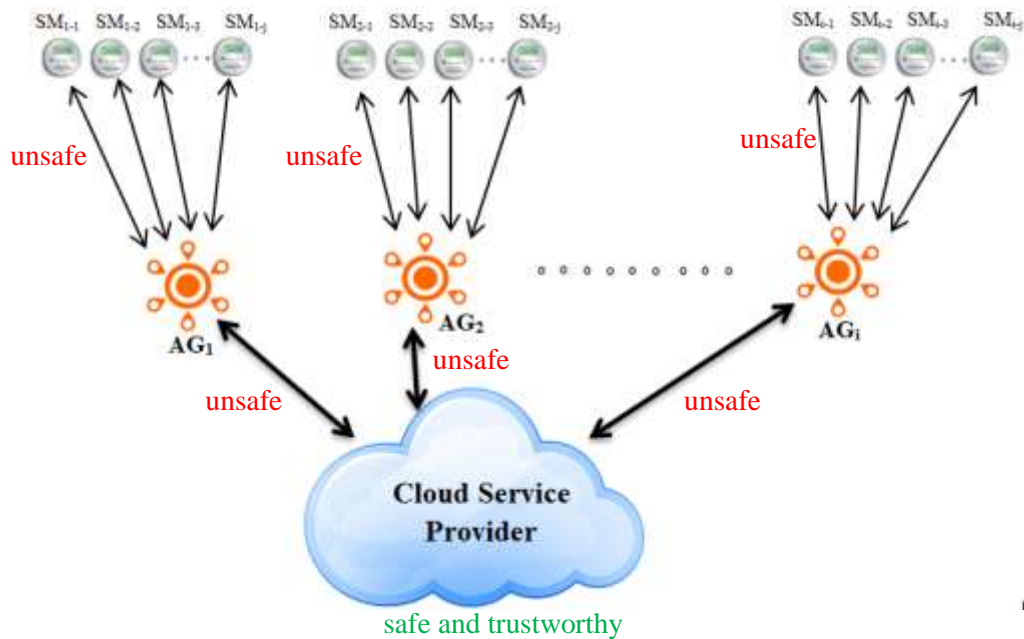


Figure 4.1- Proposed architecture of AMI in the Cloud

4.4. Adversary Model

We consider the architecture presented in Figure 4.1, where CSP implements a trustworthy private cloud, and the devices such as SM and AG cannot be manipulated physically to extract information from their systems or cloned to implement algorithms and do erroneous measurements. In addition, the channels of communication between the SMs and the AG and the channel of communication between the AGs and the CSP are considered to be **unsafe**.

Authentication protocols are a very important element for system security, particularly when the communications infrastructure is supported through public channels where attackers have many advantages to execute attacks described below:

- A man-in-the-middle (MiTM) attack can be performed between during communications between SM and AG, or between AG and CSP; this attack consists of causing the devices to believe that messages are being exchanged between authentic devices, but are being sent and received by the attacker;
- An attacker may represent an authentic device and attempt to send false information about power consumption, or may also turn an authentic device into an unknown device to avoid sending or receiving information from the system;
- It is possible for an attacker to intercept the messages of an SM to manipulate the consumption information or to intercept the messages from the AG to manipulate the two real estate consumption information of an area.

4.5. Proposed Protocol

The proposed scheme considers the aggregation of devices into groups and their simultaneous authentication. CSP serves as a trustful authority for Smart Grid and the ECDH key agreement protocol is used in the key agreement among AG/SM and the CSP. Secure channels will be drawn with arrows and unsecure ones will be drawn with dotted arrows in a graph for clarifying the characteristics of the channels through which messages are exchanged between entities.

Figure 4.2 shows an overview of the operation of the protocol described as follows:

1. A group of SMs is deployed in a specific area (neighborhood, buildings, etc.) and sends a connection request to the aggregator.
2. The aggregator groups the connection requests and sends them in a group, so that the CSP validates the identities.
3. Once the SM and AG identities have been authenticated, the CSP sends a Broadcast message to the device group (SM and AG). The message contains data for the calculation of the session keys and verification of the CSP authenticity.

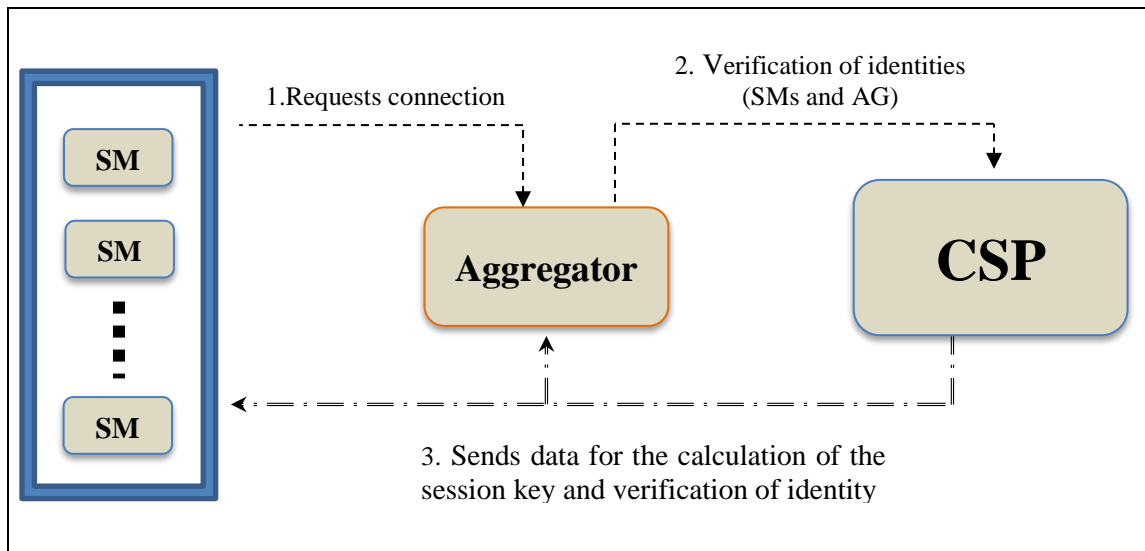


Figure 4.2 General scheme of the proposed protocol.

The protocol is composed of three phases, shown in figure 4.3:

1st phase: initialization, in which public / private master keys and group key are generated and the mathematical properties of the protocol are defined.

2nd phase: registration, in which the identity of the devices is associated with the variables calculated for the authentication process.

3rd phase: authentication, in which a group of n SMs, served by an AG, aims at authentication in an SG.

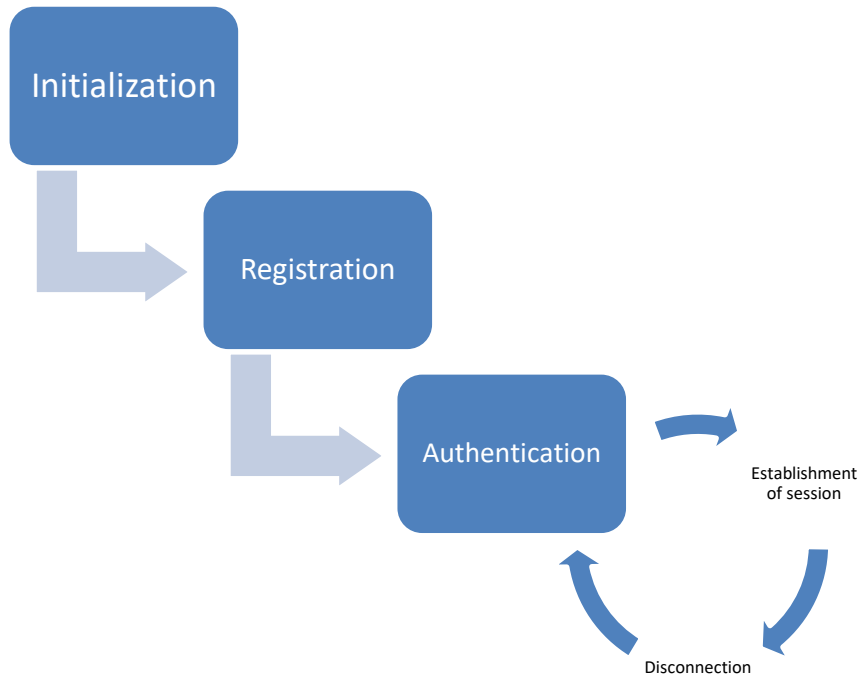


Figure 4.3- Phases and functioning of the protocol.

Below are the descriptions of the details of each phase.

1st phase: Initialization

In this phase, the CSP proceeds as follows:

- i. SMs, AG and CSP are organized into a binary tree structure, where each of them is a leaf and has an associated SECy secret value derived from the secret values of the nodes above it [12].

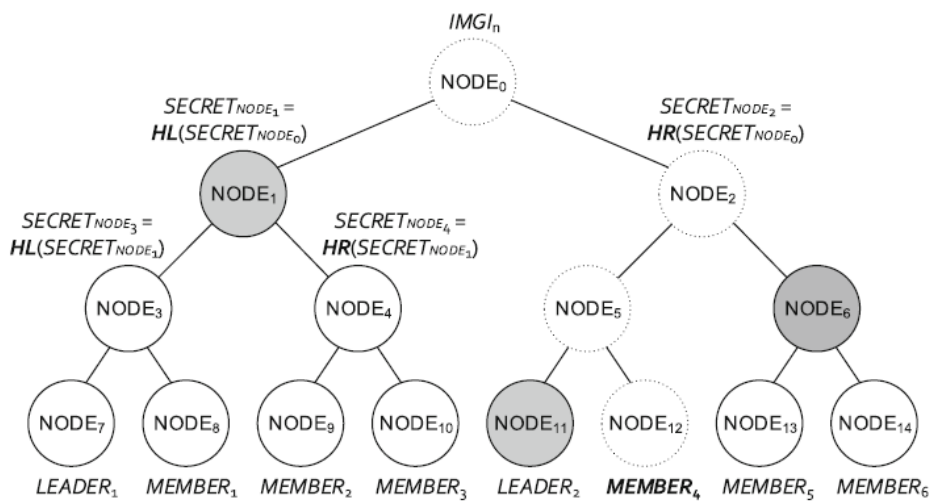
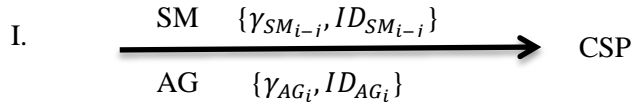


Figure 4.4- Binary tree for group organization (source: [12]).

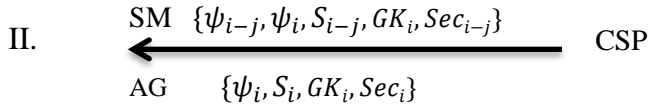
- ii. CSP chooses a random k-bits prime number and generates two elliptic curve groups, G1 and G2 of order p, and a generator point P in G1.
- iii. a random number $x_{CSP} \in Z_p^*$ is chosen as a private key and the public key is calculated as $PK_{CSP} = x_{CSP} * P$ for the generation of the master keys of the system;
- iv. the group key is calculated and generates a random number $g \in Z_p^*$ according to
$$GK_i = h_2(SEC_{i-1} \oplus SEC_{i-2} \oplus \dots \oplus SEC_{i-j} \oplus (g * PK_{CSP}))$$
- v. parameters $\{p, P, PK, G1, G2, e, h_1, h_2, h_L, h_R\}$ are published ($h_1(\cdot)$ and $h_2(\cdot)$ are hash functions, $h_L(\cdot)$ and $h_R(\cdot)$ are hash function used for the creation of the secrets of the binary tree node and $e(-,-)$, is the bilinear pairing function).

2nd phase: Registration

To register the SMs and the AGs a secure channel is used. The process for the SMs and AGs registration is described below:



AG and SM choose a random number γ_{AG_i} and $\gamma_{SM_{i-j}}$ respectively, and each of them sends a message to the CSP with the random number and device identity: $\{ \gamma_{AG_i}, ID_{AG_i} \} \{ \gamma_{SM_{i-j}}, ID_{SM_{i-j}} \}$.

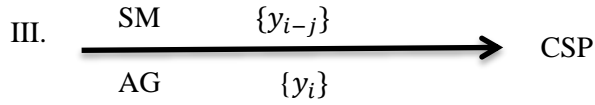


After receiving the messages, the CSP chooses a random value K_{CSP_i} and Q_i per group and calculates the authentication variables shown in table 4.1.

Table 4.1- Authentication variables

SM	AG
$r_{CSP_i} = K_{CSP_i} * P$	
$R_{SM_{i-j}} = r_{CSP_i} * \gamma_{SM_{i-j}}$	$R_{AG_i} = r_{CSP_i} * \gamma_{AG_i}$
$\psi_{i-j} = h_1(R_{SM_{i-j}} + ID_{i-j})$	$\psi_i = h_1(R_{AG_i} + ID_i)$
$S_{i-j} = x_{CSP} * \psi_{i-j} * K_{CSP_i}$	$S_i = x_{CSP} * \psi_i * K_{CSP_i}$
$Sec_{i-j} = SEC_{i-a} \oplus SEC_{i-b} \oplus \dots \oplus SEC_{i-z}$	$Sec_i = SEC_{i-a} \oplus SEC_{i-b} \oplus \dots \oplus SEC_{i-z}$

Then it generates and sends a message with such values $\{\psi_{i-j}, \psi_i, S_{i-j}, GK_i, Sec_{i-j}\}$ to each SM and $\{\psi_i, S_i, GK_i, Sec_i\}$ AG.



After receiving the message, both MS and AG calculate their public and private keys, shown in table 4.2:

Table 4.2- Private / Public keys

	SM	AG
Private Key	$x_{i-j} = s_{i-j} + \gamma_{SM_{i-j}}$	$x_i = s_i + \gamma_{AG_i}$
Public Key	$y_{i-j} = \hat{e}(x_{i-j}, P)$	$y_i = \hat{e}(x_i, P)$

Finally, the public keys of SMs (y_{i-j}) and AG (y_i) are sent back to the CSP.

The flowchart in Figure 4.5 summarizes the registration phase.

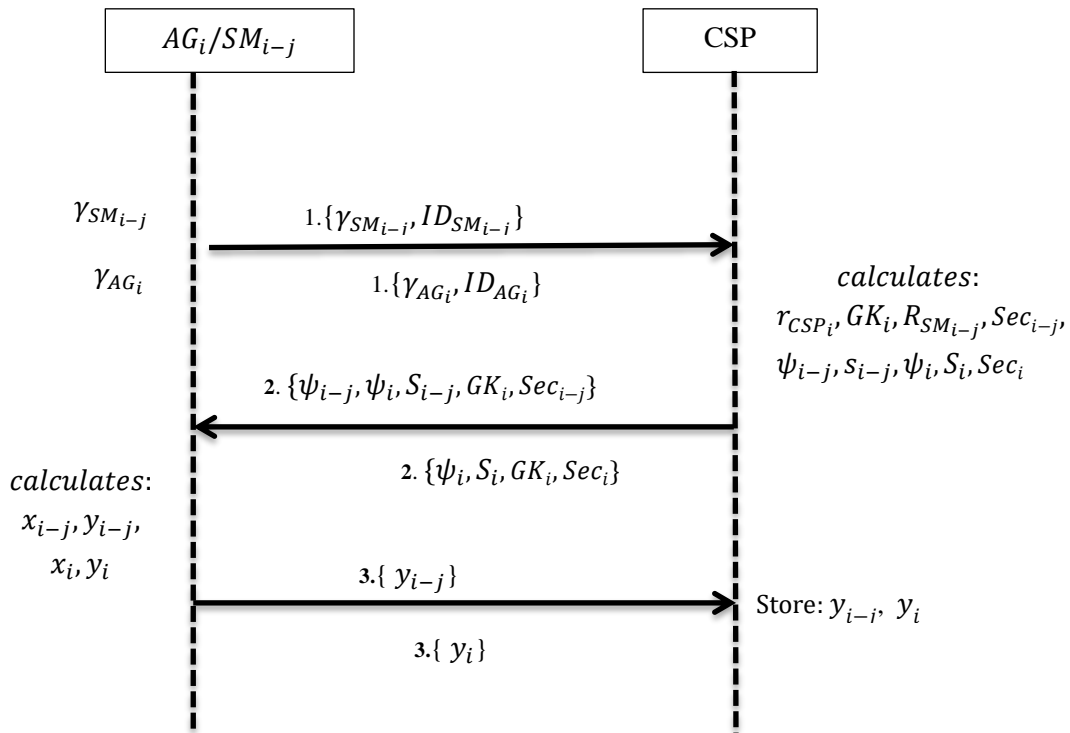


Figure 4.5- Registration phase

3rd phase: Authentication:

A group of SM_{i-j} that aims at authentication in an SG network through an AG proceeds as follows:

i. $\text{SM} \xrightarrow{\{MC_{SM_{i-j}}\}} \text{AG}$

Each SM_{i-j} chooses a random number $\sigma_{SM_{i-j}} \in Z_p^*$ and computes:

$$\begin{aligned}\lambda_{i-j} &= h_1(\sigma_{SM_{i-j}} + \gamma_{SM_{i-j}}) \\ MAC_{SM_{i-j}} &= h_2(\psi_{i-j} || |\lambda_{i-j}| | LAI_{i-j}) \\ M_{SM_{i-j}} &= (\psi_{i-j} || |\lambda_{i-j}| | LAI_{i-j} | | MAC_{SM_{i-j}}) \\ MC_{SM_{i-j}} &= M_{SM_{i-j}} \oplus (GK_i * \psi_i)\end{aligned}$$

where LAI is the Local Area Identification.

Then, each SM sends $MC_{SM_{i-j}}$ to aggregator AG_i .

ii. $\text{AG} \xrightarrow{\{AUTH_{Gi}, LAI\}} \text{CSP}$

Upon receiving the message from the other devices $\{MC_{SM_{i-j}}\}$, AG_i performs an XOR operation with its temporary identity to obtain the data of the resized message:

$$M'_{SM_{i-j}} = MC_{SM_{i-j}} \oplus (GK_i * \psi_i) = (M_{SM_{i-1}} || M_{SM_{i-2}} || \dots || M_{SM_{i-j}})$$

Once only the members of the group know the temporary group key, if the message is unreadable, an intruder is in the group and the aggregator initiates a process to search for the intruder and eliminate the connection.

Simultaneously, the aggregator chooses a number $\sigma_{AG_i} \in Z_p^*$ and, similarly to [14], calculates:

$$\begin{aligned}\lambda_i &= h_1(\sigma_{AG_i} + \gamma_{AG_i}) \\ MAC_{AG_i} &= h_2(\psi_i || |\lambda_i| | LAI_i) \\ M_{AG_i} &= (\psi_i || |\lambda_i| | LAI_i | | MAC_{AG_i})\end{aligned}$$

Otherwise, it subtracts the $MAC_{SM_{i-j}}$ messages and calculates the message authentication of the group, MAC_{Gi} :

$$MAC_{Gi} = h_2(MAC_{AG_i} \oplus MAC_{SM_{i-1}} \oplus MAC_{SM_{i-2}} \oplus \dots \oplus MAC_{SM_{i-j}})$$

Then the AG calculates a challenge L_h and generates an $AUTH_{Gi}$ message containing SM group information:

$$L_h = h_1(LAI || ID_{Gi})$$

$$AUTH_{Gi} = \left(MAC_{Gi} || M_{AGi} || M_{SM_{i-1}} || M_{SM_{i-2}} || \dots || M_{SM_{i-j}} || y_{AGi} || L_h \right)$$

AG_i finally sends $AUTH_{Gi}$ and LAI to the CSP.

iii. \leftarrow AG/SM { $AUTH_{CSP}$ } CSP

When the CSP receives the AG_i message, it checks the LAI value declared by the devices, validates the message performing $L'_h = h_1(LAI' || ID_{Gi})$ and compares $L'_h = L_h$. If the hashes do not match, the CSP sends a message to the whole failed group and terminates the authentication procedure. Otherwise, it calculates $MAC'_{AGi} = h_2(\psi_i || \lambda_i || LAI_i)$ and all $MAC'_{SM_{i-j}} = h_2(\psi_{i-j} || \lambda_{i-j} || LAI_{i-j})$ for generating the message authentication code of group $MAC'_{Gi} = h_2(MAC_{AGi} \oplus MAC_{SM_{i-1}} \oplus MAC_{SM_{i-2}} \oplus \dots \oplus MAC_{SM_{i-j}})$ and verifies if $MAC_{Gi} = MAC'_{Gi}$. If the hashes do not match, CSP sends a MAC failure message to the group. Otherwise, it verifies the authenticity of the messages sent by SMs and AG through a bilinear pairing operation, shown in table 4.3. The mathematical proof of the identity verification is shown in table 4.4.

Table 4.3. Verification of identity

SM	AG
$y_{SM_{i-j}} = \hat{e}((x_{csp} * \psi_{i-j}), r_{CSP_i}) \hat{e}(\lambda_{i-j}, P)$	$y_{AG_i} = \hat{e}((x_{csp} * \psi_i), r_{CSP_i}) \hat{e}(\lambda_i, P)$

Table 4.4. Mathematical Verification

SM	AG
$ \begin{aligned} y_{SM_{i-j}} &= \hat{e}(x_{i-j}, P) \\ &= \hat{e}(s_{i-j} + \lambda_{i-j}, P) \\ &= \hat{e}(s_{i-j}, P) \hat{e}(\lambda_{i-j}, P) \\ &= \hat{e}((x_{csp} * \psi_{i-j} * K_{CSP_i}), P) \hat{e}(\lambda_{i-j}, P) \\ &= \hat{e}((x_{csp} * \psi_{i-j}), K_{CSP_i} * P) \hat{e}(\lambda_{i-j}, P) \\ &= \hat{e}(x_{csp} * \psi_{i-j}, r_{CSP_i}) \hat{e}(\lambda_{i-j}, P) \end{aligned} $	$ \begin{aligned} y_{AG_i} &= \hat{e}(x_i, P) \\ &= \hat{e}(s_i + \lambda_i, P) \\ &= \hat{e}(s_i, P) + \hat{e}(\lambda_i, P) \\ &= \hat{e}((x_{csp} * \psi_i * K_{CSP_i}), P) \hat{e}(\lambda_i, P) \\ &= \hat{e}((x_{csp} * \psi_i), K_{CSP_i} * P) \hat{e}(\lambda_i, P) \\ &= \hat{e}(x_{csp} * \psi_i, r_{CSP_i}) \hat{e}(\lambda_i, P) \end{aligned} $

If the verification of some SMs is not satisfactory, the CSP will group its connections into a quarantine list. The satisfactory SMs are grouped into a list of connections.

If the AG verification is satisfactory, the CSP calculates the variables for the session key; otherwise, it sends an error message in the authentication to the group and closes connection.

After verifying the authentication data sent by all SMs through AG and the AG authentication data, CSP calculates a temporary group key and generates variables for the calculation of the session keys of each MS and AG

- a) CSP generates a random number r_{CSP1} , and, similarly to [14] calculates the temporary key for the group and a check value to authenticate the group:

$$GTK_i = h_1(GK_i || r_{CSP1})$$

A new group's temporary key is generated in each session.

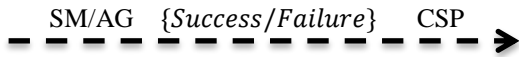
- b) Similarly to [14], the CSP chooses a random number $r_{CSP2} \in Z_p^*$ and generates variables to calculate session keys

$$F = r_{CSP2} * P$$

$$MAC_{CSP} = h_2(F || GTK_i)$$

$$AUTH_{CSP} = (F || MAC_{CSP} || r_{CSP1})$$

It then **broadcasts** $AUTH_{CSP}$ to all group members (AG_i / SM_{i-j}).



- c) Similarly to [14], when SM_{i-j} and AG_i receive the message, they compute

$$GTK_i = h_1(GK_i || r_{CSP1})$$

$$MAC'_{CSP} = h_2(F || GTK_i)$$

Then, they check if $MAC_{CSP} = MAC'_{CSP}$. If the verification fails, they send a MAC failure message to the CSP; otherwise, the CSP is authenticated by the devices.

At the end of the authentication phase, the CSP is bound to the binary tree as a leaf and an SECY secret value is associated, as shown in Figure 4.6 [12].

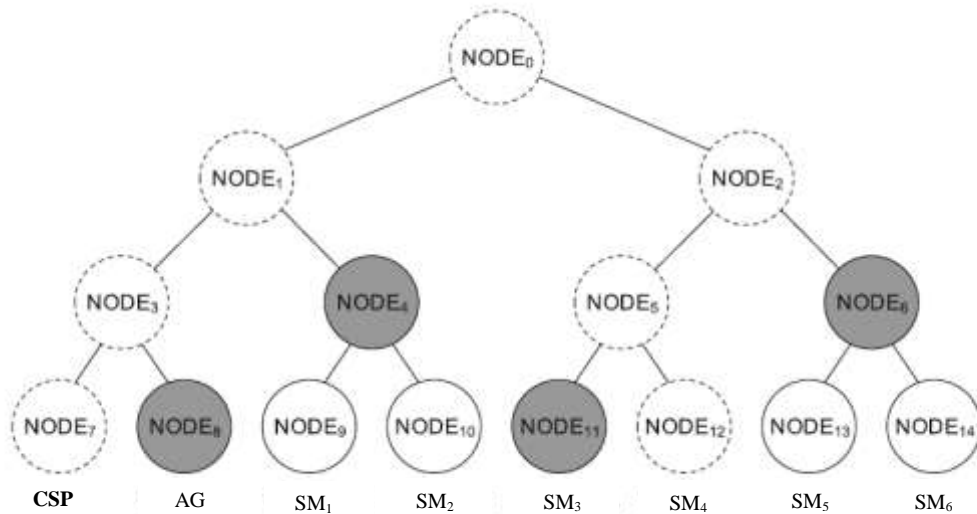


Figure 4.6 – Binary tree after the entrance of CSP (source [12]).

CSP and AG_1 / SM_{i-j} compare the secret they know and find out what secrets they have in common. For example, the gray circles in Figure 4.6 represent the common values of CSP and SM_4 [12]. When the common secrets are identified between SM / AG and the CSP, the calculation of the session key is initiated (see Table 5).

Table 4.5- Session key generation

Session Key AG	$SK_{i-CSP} = ((SEC_a \oplus SEC_b \oplus \dots \oplus SEC_z) * \lambda_i * F)$
Session Key SM	$SK_{i-j-CSP} = ((SEC_e \oplus SEC_f \oplus \dots \oplus SEC_w) * \lambda_{i-j} * F)$

where $SEC_a, SEC_b \dots SEC_z$ and $SEC_e, SEC_f \dots SEC_w$ are the common secret values of AG_i / SM_{i-j} and CSP , respectively. This model of session key is based on the session key presented by *Choi et al.*[11] and can be used for device-to-device communication (D2D) among SSM_{i-j} , AG_i and CSP_i . The entire Key Agreement and Key Distribution process is shown in Figure 4.7.

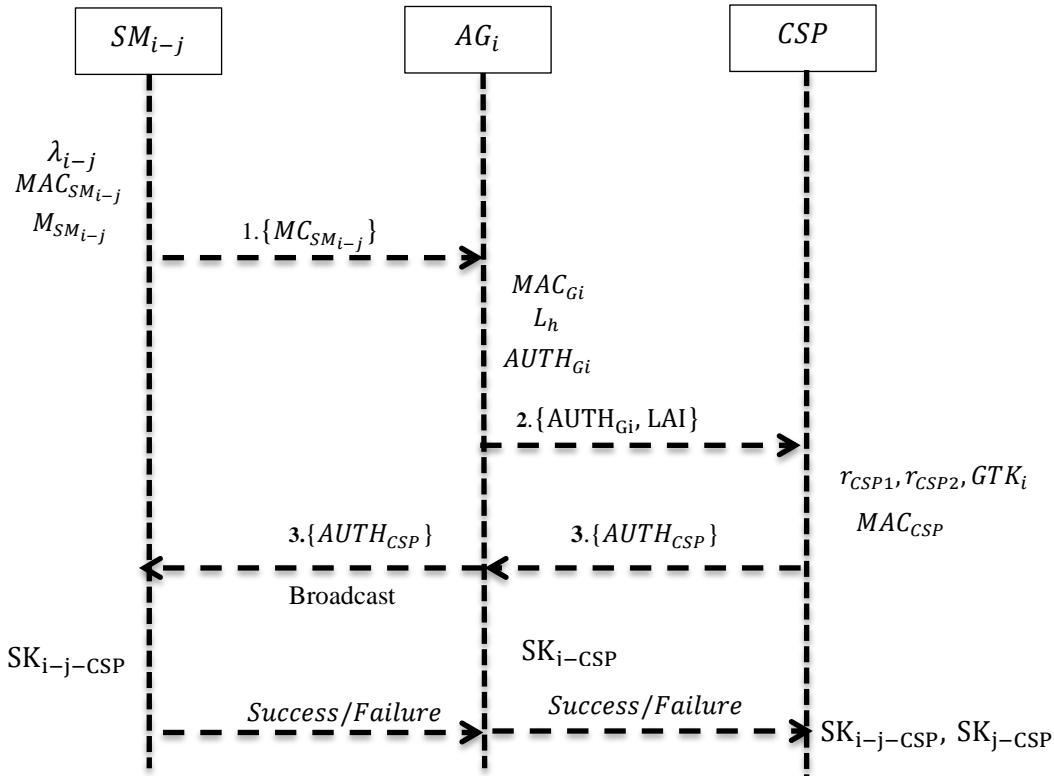


Figure 4.7- Authentication Phase

Whenever a device is added or leaves the group, the group key must be updated to ensure backward secrecy and forward secrecy [11,13].

If a new device wishes to join the group, it must be attached to the binary tree and, depending on the place, the member will have a secret SEC_{i-y} associated. A new group key is then calculated with this secret:

$$GK'_i = h_3(GK_i \oplus SEC_{i-y})$$

If a device leaves the group, the new group key is calculated as follows:

$$GK''_i = GK_i \oplus SEC_{i-y}$$

The execution of the hash function is not necessary, and the device leaving the group cannot calculate the new group key, because a single hash operation prevents the group key from being reversed to the old group keys.

4.6. Security Analysis

This section reports on an analysis of the proposed protocol which considered security properties.

- **Mutual Authentication:** In the first message, the SM sends data to be authenticated in the system to the AG, that data is encrypted with the initial group key (GK_i) multiplied by the AG signature, so that only an authentic AG can un-message the message, on the other side, if the AG can un-mute the message, it confirms that the SM is authenticated and is part of the group.

In the second message, the AG and SMs authentication data are sent to the CSP, which performs a bilinear pairing operation to check if the entities that sent the data are authentic.

In the third message, the CSP sends data through Broadcast to the AG and the Evs that are part of the group, with this data both SM and AG verifying that the CSP that sends the message is authentic.

- **Confidentiality and Integrity:** Messages exchanged among SM, AG, and CSP are protected by encryption with a session key, generated at the end of the authentication process, combined with a hash function on each message so the receiver of the message can verify the integrity of the messages, guaranteeing its confidentiality and integrity.
- **Privacy (Anonymity):** Each SM and AG has a temporary identity (λ_{i-j}). Additionally, only the CSP can know their permanent identities (ID). If an attacker intercepts a message, it will obtain only its temporary identities, therefore, the privacy of the system is guaranteed.
- **Perfect FS/BS:** The group key is updated whenever a member enters or leaves. If a new member joins the group, it cannot access the old messages, because the group key has been updated. If a member leaves the group, it will not be able to access the group messages, because the group key has been updated.
- **Replay Attack:** Once all entities generate random values for the calculation of some values during the authentication process, an attacker cannot obtain information from the messages using old data.
- **DoS Attack:** Value L_h is very important for the verification of the authenticity of the devices and avoidance of DoS attacks, once only if L_h is valid, the CSP checks the MAC of the group. DoS attacks are also mitigated with the implementation of a challenge in the protocol.

- **Man-in-the-Middle attack:** The session key cannot be calculated from intercepted information from the communication channel, because its calculation is based on binary tree secret values and ECDH encryption techniques. Group keys GK and GTK cannot be calculated either, because they are not exposed in any message.
- **Redirection attack:** Each SM and AG includes the LAI for calculating their *MAC* and the *CSP* can check if it is a valid LAI. If an attacker tries to forge the LAI, the verification of $MAC_{SM_{i-j}}$ fails and the redirection attack is avoided. In the SM case, this attack is mitigated with the implementation of challenge and response in the protocol.
- **Known key attack:** The protocol is resistant to this attack, because each session has a different key calculated from random values.
- **Impersonation attack:** The device and group identities are not revealed, therefore, an attacker cannot impersonate them. *CSP* cannot generate public keys of entities if a value sent is wrong.

4.7. Formal Verification of the Proposed Protocol

AVISPA tool was used for the formal security verification of the protocol, once it is considered reliable for the security evaluation of protocols [7].

Figures 4.8, 4.9 and 4.10 show parts of the HLPSL codes used for modeling the behavior of the protocol.

4.7.1. Protocol Simulation

The entity modeling in the HLPSL language consists of the following 3 parts:

- i. Declaration of system elements: agents, channels and constants known by the entity, temporary variables and declaration of the functions to be used.
- ii. State Creation: states describe operations and messages that must be exchanged with other entities and are differentiated by number assignment.
- iii. Declaration of secrets: at the end of each State, the elements that must be kept secret are declared.

Figure 4.8 shows the HLSPL language that models the behavior developed by SM.

```

role role_SM(SM,AG,CSP:agent,P,IDSsm,IDg,TIDsm,TIDag,TIDg,GK,SEC1,SEC2:text,SND1,RCV1,RCV3:channel(dy))
played_by SM
def=
    local
        State:nat,
        Rij,LAIsM,MACcsp,MACij,GTK,Rcsp2,Rcsp1,Msm,MC,Aij:text,
        H2,M,Sum:function,
        SKij:symmetric_key

    init
        State := 0

    transition
        1. State = 0  $\wedge$  RCV1(start) => State':=1
            $\wedge$  secret(IDg',sec_6, {})
            $\wedge$  secret(IDsm',sec_5, {})
            $\wedge$  Rij' := new()
            $\wedge$  LAIsM' := new()
            $\wedge$  Aij' := Sum(P,Rij')
            $\wedge$  MACij' := H2(Aij'.TIDsm,LAIsM)
            $\wedge$  Msm' := Aij'.MACij'.TIDsm.LAIsM
            $\wedge$  MC' := xor(Msm',M(GK,TIDag))
            $\wedge$  secret(IDsm',sec_2, {})  $\wedge$  secret(Rij',sec_3, {})  $\wedge$  SND1(MC')

        6. State=1  $\wedge$  RCV3(M(P,Rcsp2').Rcsp1'.MACcsp') => State':=2
            $\wedge$  secret(GTK',sec_7, {})
            $\wedge$  SKij' := M(M(xor(SEC2',SEC1'),Aij'),H2(M(P',Rcsp2')))
            $\wedge$  secret(SKij',sec_1, {})

end role

```

Figure 4.8- Role of each User in HLSPL.

Figure 4.9 shows the role session that describes, in HLSPL language, the establishment of the session and the environment where the protocol will be run. An important part of this section refers to the stability of system information (variants, keys, agents, etc.) that can be intercepted by the attacker in some undetermined way.

```

ole session1(SM,AG,CSP:agent,
             TIDsm,TIDag,P,IDSsm,IDg,TIDg,IDag,SEK,GK,Yag,SEC1,SEC2,SEC3,SEC4:text,
             SND1,RCV1,SND2,RCV2,SND3,RCV3,SND4,RCV4:channel(dy))
def=
    composition
        role_SM(SM,AG,CSP,P,IDSsm,IDg,TIDsm,TIDag,TIDg,SEC1,SEC2,GK,SND1,RCV1,RCV3)
         $\wedge$  role_AG(SM,AG,CSP,P,IDg,TIDg,IDag,TIDsm,TIDag,Yag,SEC3,SEC4,GK,SND2,RCV1,RCV3,SND4)
         $\wedge$  role_CSP(SM,AG,CSP,P,IDSsm,IDg,TIDag,TIDsm,TIDg,SEC1,SEC2,SEC3,SEC4,GK,SND3,RCV2,RCV4)
    end role

    role environment()
    def=
        const
            idsM,idg,tidg,sec1,sec2,sec3,sec4,p,tidag,tidsM,idag,sek,gk,yag:text,
            sm,csp,ag:agent,
            sec_1, sec_2,sec_3,sec_4,sec_5,sec_6,sec_7:protocol_id,
            snd1,rcv1,snd2,rcv2,snd3,rcv3,snd4,rcv4 : channel (dy),
            sec_10:symmetric_key

            intruder_knowledge = {}

        composition
            session1(sm,ag,csp,tidsM,tidag,tidg,sec1,sec2,p,idsM,idg,idag,sek,gk,yag,sec3,sec4,snd1,rcv1,snd2,rcv2,snd3,rcv3,snd4,rcv4)
             $\wedge$  session1(i,ag,csp,tidsM,tidag,tidg,sec1,sec2,p,idsM,idg,idag,sek,gk,yag,sec3,sec4,snd1,rcv1,snd2,rcv2,snd3,rcv3,snd4,rcv4)
             $\wedge$  session1(sm,i,csp,tidsM,tidag,tidg,sec1,sec2,p,idsM,idg,idag,sek,gk,yag,sec3,sec4,snd1,rcv1,snd2,rcv2,snd3,rcv3,snd4,rcv4)
             $\wedge$  session1(sm,ag,i,tidsM,tidag,tidg,sec1,sec2,p,idsM,idg,idag,sek,gk,yag,sec3,sec4,snd1,rcv1,snd2,rcv2,snd3,rcv3,snd4,rcv4)
        end role
    end role

```

Figure 4.9- Role specification for the session and environment in HLSPL.

Finally, Figure 4.10 shows the security objectives of the protocol and the definition of the secrets declared in the entities, namely device location, random variables for the calculation of the session key, initial and temporary group keys, SM and AG identities, described below:

secrecy_of sec_1: represents the session key SK_{ij} , which in the end can only be known by the SM and the CSP.

secrecy_of sec_2: represents the identity of the SM (ID_{sm}), which can only be ascertained by the SM and SAS.

secrecy_of sec_3: represents the random value of SM $\gamma_{SM_{i-j}}$, used for authentication and private key generation, the public key and the session key.

secrecy_of sec_4: represents the session key SK_i , which in the end can only be known by the AG and the CSP.

secrecy_of sec_5: represents the identity of the AG (ID_{AG}), which can only be ascertained by the AG and SAS.

secrecy_of sec_6: represents the random value of AG γ_{AG_i} , used for authentication and private key generation, the public key and the session key.

secrecy_of sec_7: represents the temporal group key GTK_i , which in the end can only be known by the SM, AG and the CSP.

```

goal
  secrecy_of sec_1
  secrecy_of sec_2
  secrecy_of sec_3
  secrecy_of sec_4
  secrecy_of sec_5
  secrecy_of sec_6
  secrecy_of sec_7
end goal
environment()

```

Figure 4.10- Security goals established in HLSPL

4.7.2. Results of Security Verification

The protocol was verified through a simulation of its behavior with two back ends, i.e., OFMC and CL-AtSe, by AVISPA tool. The results (Fig. 4.11) showed it is safe for both back-ends.

<pre> % OFMC % Version of 2006/02/13 SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS PROTOCOL /home/span/span/testsuite/results/artigo_2_v11.if GOAL as_specified BACKEND OFMC COMMENTS STATISTICS parseTime: 0.00s searchTime: 3.30s visitedNodes: 632 nodes depth: 6 plies </pre>	<pre> SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS TYPED_MODEL PROTOCOL /home/span/span/testsuite/results/artigo_2_v11.if GOAL As Specified BACKEND CL-AtSe STATISTICS Analysed : 15 states Reachable : 15 states Translation: 0.08 seconds Computation: 0.05 seconds </pre>
a) OFMC back-end	b) CL-AtSe back-end

Figure 4.11- Results of a security simulation for OFMC and CL-AtSe.

Figure 4.11.a) shows the results of the simulation of the proposed protocol HLPSL code applying the OFMC backend. In the summary section indicates that the protocol is **safe**. In the statistics part, we can also see that the search time was 3.30 seconds, the number of nodes visited was 632 and the depth was 6.

Figure 4.11.b) shows the simulation results of the proposed protocol HLPSL code applying the CL-AtSe backend. In the summary part you can see that the protocol is **safe**. In the statistics part, we can also see that 15 states were analyzed, and 15 states were reached, the translation took 0.08 seconds and the computation was 0.05 seconds.

4.7.3.Simulation of intrusion with SPAN

To better visualize the iteration between the entities of the analyzed protocols the AVISPA developers have created a Web tool called AVISPA (SPAN) security protocol Animator. SPAN design messages exchanged between entities, in addition, has the ability to simulate the attacks found in the protocol analyzed and in case the protocol analyzed is secure it can simulate iteration that may have intruder in the protocol.

As a result of which the proposed protocol was analyzed as safe by AVISPA, only the simulation was performed where the proposed protocol interacts with an attacker. Figure 4.12 shows the simulation of an attacker between MS and AG and Figure 4.13 shows the simulation of the proposed protocol interacting with an intruder between the AG and the CSP.

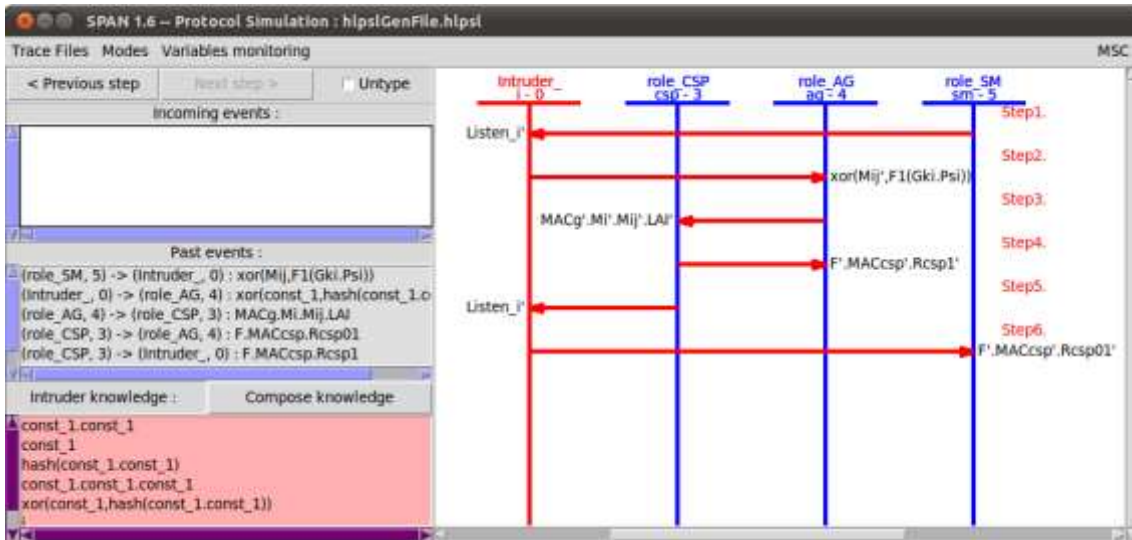


Figure 4.12- Intrusion simulation between SM and AG with SPAN

Figure 4.12 shows the behavior of the proposed protocol before an attacker located between SM and AG that can execute the following attacks:

i. Impersonation Attack

An attacker can execute a proxy attack between SM and AG as long as they know the group key, in case of getting the group key the attacker can execute a proxy attack in two scenarios:

Scenario 1: An attacker may try to represent a valid SM and change the certificate ψ_{i-j} , but AG will check the integrity of the message with the MAC_{i-j} of the message, think it was modified, and terminate the connection.

Scenario 2: An attacker can change the ψ_{i-j} and MAC_{i-j} of the message and send the message to the CSP to verify the identity, but the attacker cannot generate a ψ_{i-j} of a valid user because he does not know the $\gamma_{SM_{i-j}}$, nor the identity of the user ID_{i-j} , nor the random value generated by the server K_{CSP_i} , therefore the CSP would not be able to identify this SM and would end the communication with him.

ii. MITM Attack:

An attacker can intercept messages between SM and AG to subtract information to gain access to the system. In Figure 4.12 you can look at an attacker who establishes a communication with SM and another with AG. The MiTM attack can be performed in three scenarios:

Scenario 1: An attacker can try to change the MC_{ms} , but since she does not know Gk_i , then AG tries to decipher the message and finds that the message is unreadable so it has changed and the connection is terminated.

Scenario 2: In case the attacker knows Gk_i and gets SM information (M_{i-j}), the attacker will not be able to obtain SM confidential information ($ID_i, x_{SM_{i-j}}$).

Scenario 3: An attacker may attempt to extract some information from message-3, but can not generate a certain session key because it does not know the secrets of the binary tree ($SEC_a \oplus SEC_b \oplus \dots \oplus SEC_z$).

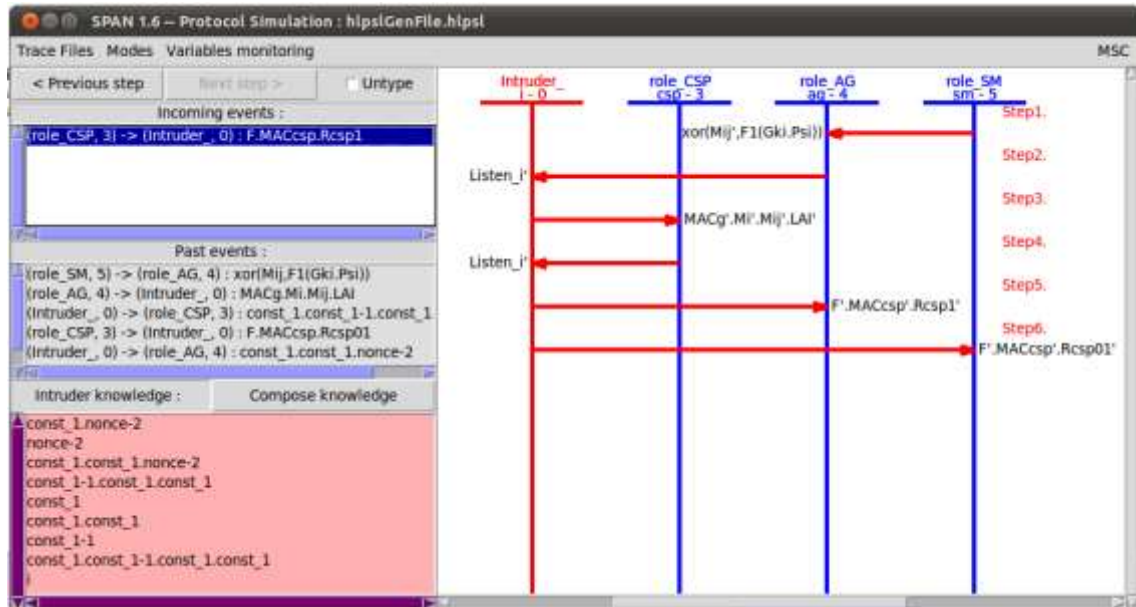


Figure 4.13- Intrusion simulation between AG and CSP with SPAN

Figure 4.13 shows the behavior of the proposed protocol before an attacker located between the AG and the CSP. An attacker can execute the following attacks:

i. Impersonation Attack:

In this attack an attacker may attempt to pass a valid user. In Figure 4.13 there are two scenarios where a personification attack can be performed:

Scenario 1: An attacker may attempt to change the AG ψ_i certificate, but the CSP will check the message integrity of the group MAC_G and MAC_i of the AG data, find that it has been modified, and terminate the connection.

Scenario 2: an attacker can change the ψ_i , the MAC_i do AG and the MAC_G the group message and send the message to the CSP to verify the identity, but the attacker cannot generate a ψ_i , of a valid AG because it does not know the generated random value by the user γ_{AG_i} , nor the identity of the user ID_i , nor the random value generated by the server K_{CSP_i} , therefore the CSP would not be able to identify this SM and would end the communication with it.

ii. MITM Attack:

An attacker can intercept messages between the AG and the CSP to subtract information to gain access to the system. In Figure 4.Y you can look at an attacker who establishes communication with the AG and another with the CSP. The MITM attack can be performed in three scenarios:

Scenario 1: If the attacker knows Gk_i , he can group the messages, but he does not get information from the users, nor does he generate the session key, besides, he can not generate a certain M_{AG_i} , since LAI_i is different from LAI_{attack} of the attacker.

Scenario 2: In case the attacker trying to represent an AG knows the Gk_i and clones the right LAI_i , it can not generate a certain ψ_i because it does not know the random value generated by the user γ_{AG_i} , nor the identity of the user ID_i , nor the random value generated by the server K_{CSP_i} .

Scenario 3: In case the attacker trying to represent an AG, knows the Gk_i and clones the right LAI_i and uses a ψ_i of a certain AG, CSP will generate the values so that group members can generate the session key, but the attacker can not generate a certain session key because it does not even know the secrets of the binary tree ($SEC_a \oplus SEC_b \oplus \dots \oplus SEC_z$).

4.8. Performance Evaluation

This section addresses the evaluation of the performance of the protocol and its comparison to the protocols designed by Wan et al. [3] and Nicanfar et al. [7].

4.8.1. Communication Cost

The values taken from Saxena et al. [13] and shown in Table 6 were used for the comparison of the communication costs.

Table 4.6- Communication cost of each parameter transmitted [13].

Parameter	Size (bits)	Parameter	Size (bits)
ID/TID	128	Ti	32
ECDH	192	Hash	128
MAC	64	LAI	40
PAIRING	192	SN(Serial)	32

An environment with n devices per aggregator was considered and the calculations were based on the number of bits per parameter exchanged in each message. Table 7 shows the computational costs of our protocol and the protocols of Wan et al. [3] and Nicanfar et al. [7] with n SMs.

Table 4.7- Communication costs in bits per message and total.

	M1	M2	M3	M4	TOTAL
Wan et al.[3]	192n	448n	64n	192n	864n
Nicanfar et al. [7]	352n	640n	256n	-	1248n
Proposed	360n	360n + 656	384	-	720n + 1040

According to Table 7, the protocol of Nicanfar et al. [7] requires a very high communication cost in both bits and transmitted messages in comparison to our scheme. On the other hand, the protocol proposed by Wan et al. [3] showed better performance regarding number of messages transmitted, if $SM \leq 8$. Our protocol performs better for groups with $SM > 8$. However, concerning number of transmitted bits, the protocol of Wan et al. [3] showed better performance with $SM < 2$, and for groups with $SM > 2$ our protocol showed better performance.

The graph in Figure 4.14 shows a comparison of the communication costs of our protocol and the protocols of Wan et al. [3] and Nicanfar et al. [7]. A linear growth in the costs, related to an increase in the number of authenticated SMs is observed. Our protocol considers the use of aggregators in the AMI architecture for grouping authentication data of the SM's and to send less messages to the CSP in order to perform an authentication process of each member of the group, thus contributing to reduce communication costs in the authentication phase of the protocol.

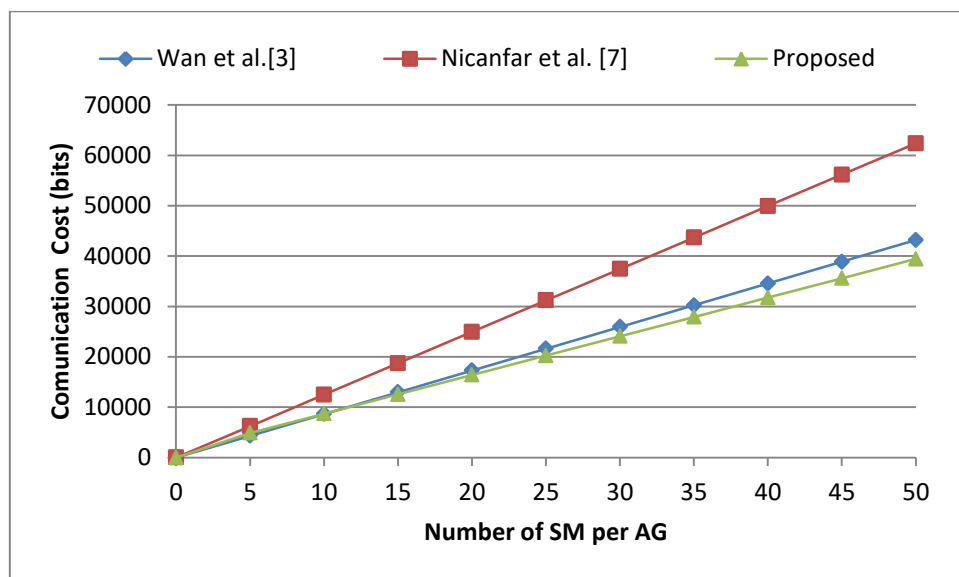


Figure 4.14- Communication Costs of the Protocols

4.8.2. Computational Cost

The computational costs adopted in Wan et al. [3] were used for the quantification, analyses and comparison of the computational costs of the three protocols. The authors used a device called MICAZ of 4KB RAM, 128KB ROM and a microprocessor working at 7.3 MHz to simulate the hardware of an SM, and Pentium IV 3-GHz desktop for simulating MDMS hardware. Table 4.8 shows the computational costs and nomenclature of the functions. Mathematical operations XOR, hash, MAC, encryption / decryption and addition are not considered for SAS, MDMS and CSP entities, due to their insignificant execution time.

Table 4.8- Nomenclature used and time spent on each operation [3]

Notation	Execution Time (ms)		Description
	SM/AG	SAS/MDMS/CSP	
T_{hash}	0,023	--	Cost of a one-way hash operation
T_{mul}	2,45	1,82	Cost of a multiplication operation over elliptical curve
T_{MAC}	0,023	--	Cost of a MAC operation
T_{pair}	5,32	3,88	Cost of a bilinear pairing operation
T_{exp}	2,45	1,82	Cost of modular exponentiation
$T_{en/de}$	0,023	--	Cost of encryption or decryption
T_{add}	0,023	--	Cost of modular addition
$T_{hash-key-nodes}$	2,45	1,82	Cost of each hash-key of all nodes

According to Table 4.9, the proposed protocol, which performed the largest number of operations in the cloud (which has superior computational resources in comparison to the other entities) showed better performance and flexibility in the AMI infrastructure and avoided the overloading of devices with limited computational resources.

Table 4.9- Comparison of the computational costs of the protocols for the generation and distribution of keys in the devices

Protocol	SM's	AG	MDMS/SAS/CSP
Wan et al. [3] Protocol	$nT_{pair} + nT_{mul} + nT_{hash} + nT_{MAC} + nT_{add}$	-	$2T_{pair}(n) + 2T_{mul}(n)$
Nicanfar et al.[7] Protocol	$3nT_{exp} + 2nT_{mul} + 10nT_{hash} + 4Tn_{en/de}$	-	$3T_{exp}(n) + 2T_{mul}(n)$
Proposed Protocol	$3nT_{mul} + 2nT_{MAC} + 2nT_{hash}$	$3T_{mul} + 4T_{MAC} + 2T_{hash}$	$(3n + 4)T_{mul} + (n + 1)T_{pair}$

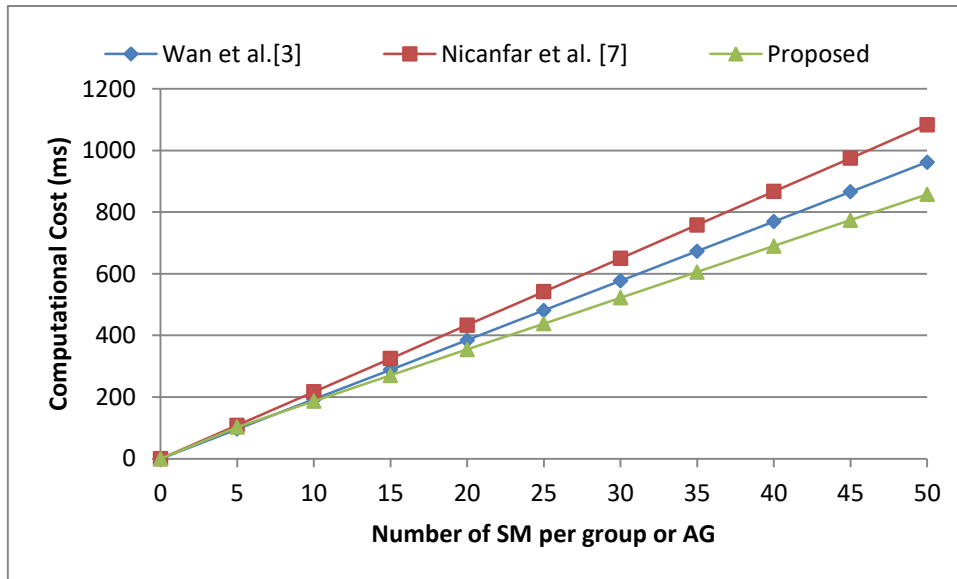


Figure 4.15- Comparison of computational costs among the protocols

According to Figure 4.15, the proposed protocol shows the best computational cost when more than 4 SM are connected to an aggregator. It uses aggregators in the AMI architecture with security and performance features. Regarding security, the aggregator checks the MACs of messages sent by SMs and also performs the authentication process, which guarantees its reliability in the system. Concerning computational performance, it groups the data and sends them to the CSP, which concomitantly checks the data of all SM, thus reducing the computational costs of the system.

4.9. Conclusions and Future Work

Information technologies are fundamental for the evolution of public infrastructures, including electrical networks, and have given rise to a new generation of electric grids, called Smart Grid.

In Smart Grid, the Advanced Measurement Infrastructure integrates several elements that enable bidirectional communication between smart meters and utility systems. One of AMI's challenges is to support two-way communication and real-time data processing of millions of devices. One of the technologies that can handle such challenges is cloud computing. Among the many advantages it offers are reliability, high availability, integrity, scalability and performance, which make it a strong candidate to support AMI applications. However, its utilization requires security protection

AMI possess a critical role in SG, so its security is of particular importance and must guarantee the integrity, confidentiality and availability of the infrastructure.

This chapter introduced a new group authentication protocol for the AMI network integrated with the cloud and based on ECDH and bilinear pairing.

The chapter began with a brief description of some works in the context of integration of Smart Grid with the cloud and other works that proposed solutions for the authentication in AMI networks.

In the proposed protocol, a simultaneous authentication scheme of a group of devices in an AMI architecture integrated with the cloud is developed; in addition, the proposed protocol guarantees the integrity, confidentiality and privacy of the user data.

In comparison with the protocol designed by Nicanfar et al. [7], our protocol shows better computational and communication costs and, compared with that of Wan et al. [3], it showed the lowest number of messages exchanged for groups of $SM > 2$ and a smaller number of bits transmitted for groups of $SM > 8$. Moreover, it offered a better computational cost in groups larger than four SM's.

The optimal performance of the proposed protocol is due to several factors such as: the use of the aggregator that groups the communications and allows the simultaneous verification of SM, to efficiently use the variables created for the authentication and to execute the operations that need more processing in the entity with better computing resources. The proposed scheme proves to be an excellent solution for IoT authentication problems and low cost computational schemes.

Finally, we observe that the proposal of more secure authentication that do not incur high processing power or high bandwidth needs is of special importance for a communication between smart meters and aggregators and control center that is more resistant to external and internal invaders.

Future work includes treatment of non-uniform groups with different numbers of smart meters per aggregators, integration with 5G networks, as well as discussions related to storage and verification costs. In addition, work on computational trust must be performed.

4.10. References

- [1] Energy-Related Services In Smart Public Infrastructures”. *Computers in Industry*, v. 88, p.35-43, 2017.
- [2] Bera, S., Misra, S., Rodrigues, J. J. P. C. "Cloud Computing Applications for Smart Grid: A Survey". *IEEE Transactions on Parallel and Distributed Systems*, v. 26, n. 5, pp. 1477-1494, 2015.
- [3] Wan, Z., Wang, G., Yang, Y., Shi, S. "SKM: Scalable Key Management for Advanced Metering Infrastructure in Smart Grids". *IEEE Trans. Ind. Electron.*, vol. 61, no. 12, pp. 7055-7066, Dec. 2014.
- [4] Genge, B., Beres, A., Haller, P. “A Survey On Cloud-Based Software Platforms To Implement Secure Smart Grids”. *49th Universities Power Engineering Conference - UPEC2014*, 2014.
- [5] Ye, F., Qian, Y., Hu, R.. “An Identity-Based Security Scheme for a Big Data Driven Cloud Computing Framework in Smart Grid”. *Global Communications Conference*, 2015
- [6] Saxena, N., Grijalva, S., “Dynamic Secrets and Secret Keys Based Scheme for Securing Last Mile Smart Grid Wireless Communication”. *IEEE Transactions on Industrial Informatics*, v. 13, n 3, 2017.
- [7] Nicanfar, H., Jokar, P., Beznosov, K. and Leung, V. “Efficient Authentication and Key Management Mechanisms for Smart Grid Communications”. *IEEE Systems Journal*, v. 8, n 2, 2013.
- [8] Butun, I., Erol-Kantarci, M., Kantarci, B., and Song, H. “Cloud-centric Multi-Level Authentication as a Service for Secure Public Safety Device Networks”. *IEEE Communications Magazine*, v. 54, n 4, 2016.
- [9] Stallings, William. “Cryptography and Network Security: Principles and Practice”. sixth ed. Boston: Pearson, 2014.
- [10] The AVISPA Project: European Union in the Future and Emerging Technologies (FET Open). Retrieved Nov 26, 2016, from <http://www.avispa-project.org>.
- [11] Cremers, C. J. F. and Feltz, M. Beyond eCK: “Perfect Forward Secrecy Under Actor Compromise and Ephemeral-key Reveal”. *Designs, Codes and Cryptography*, v. 74, n. 1, p. 183–218, 2015.
- [12] Choi, D., Hong, S. and Choi, H.K. “A group-based security protocol for Machine Type Communications in LTE-Advanced”. *Wireless Network*, v. 21, n. 2, p.405-419, 2015.
- [13] N. Saxena, B. Choi, and B. Lu, “Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid”. *IEEE Transactions On Information Forensics And Security*. v.11, NO.5.
- [14] A. P. Golembiouski Lopes, L. Oliveira Hilgert, “Group Authentication Protocols for Internet of Things (IoT) – QoS and Security Properties Evaluation”, Graduation Work, Faculty of Technology, Universidade de Brasilia, 2016.

Chapter 5

Authentication Protocol for Vehicle to Grid Networks in Smart Grid

Resumo:

Abstract: *The Vehicle to Grid (V2G) network is a very important component for Smart Grid (SG), as it can offer new services that help the optimization of both supply and demand of energy in the SG network. However, the privacy and anonymity of the users' identity, confidentiality of the transmitted data and location of the Electric Vehicle (EV) must be guaranteed. This chapter proposes a pairing-based authentication protocol that guarantees the anonymity of users and confidentiality of communications and prevents the tracking of the vehicle. The results from computational and communications performance analyses are better in comparison to other protocols.*

5.1. Introduction

Smart Grid has been developed as the next generation of energetic infrastructure. The mixture of the current electrical network and information technologies enables both clients and enterprises to participate in the monitoring management and energy distribution for a better demand-response balance.

Electric Vehicles (EVs) have been one of the most researched topics over the past years and can be easily integrated as part of a Smart Grid infrastructure. They have gained popularity towards reducing the air pollution (17% of the CO₂ global emissions) caused by fuel-operated vehicles. Studies have indicated 70% of the CO₂ emissions might be reduced if EVs were used to replace vehicles powered by traditional fuels [1].

An important part of EVs is their battery, considered a promising means of energy storing. They are stable storing units (their energy-loss rate is low) of fast charge and discharge, therefore, their integration with traditional energy plants is feasible for balancing changes in electricity demands. For instance, if the electricity demand increased, EVs would rapidly provide electricity from their batteries to the network and if it decreased, they could rapidly store the extra energy of the network. Such an interaction between EVs and Smart Grid occurs through a bidirectional communication called Vehicle-to-Grid (V2G) [2-5].

V2G communication systems display special characteristics, as vehicle mobility [6], geographic location of the vehicle, charge and discharge operations [7], conduction pattern, among others. Several security and privacy challenges in communications can affect the V2G system, therefore, confidential information, as identity of the vehicle, user's identity, identification of

the charging station, type of vehicle, time of charge and discharge, and localization of the vehicle must be protected.

An EV has two operation modes, namely home and visiting. The home mode refers to stations in the geographic area of a home area network where the vehicle resides and is registered, whereas the visiting mode includes stations outside of the residence area and is served by a visiting area network of the vehicle. Both modes have different security requirements ([5], [8-11]).

On the other hand, privacy and confidentiality are two very important concepts for informatics security. Private information must be kept confidential, which is one of the great challenges of V2G and Smart Grid networks. Every SG network is vulnerable to attacks to its different components, from EVs to CC, therefore, security measures must comprehend the entire SG network infrastructure for ensuring availability, integrity, confidentiality and non-repudiation. However, some attacks may occur, such as replication, spoofing / sniffing of payload, Denial of Service (DoS) and Man-in-the-Middle attacks.

An authentication protocol is fundamental in the V2G networks for guaranteeing only authorized EVs can access them. Therefore, an effective and efficient authentication system is highly required for guaranteeing privacy and confidentiality of data in V2G networks [12-15].

This chapter proposes a group authentication protocol for the administration and distribution of keys in a V2G architecture. The protocol is based on groups for managing secret keys, Elliptic Curve - Diffie Hellman (ECDH) for sharing secrets and bilinear pairing for providing authentication and generation of simultaneous and efficient session keys for EVs grouped under aggregators.

The remainder of the chapter is organized as follows: Section 2 describes some works related to the authentication of EV in the V2G network; Section 3 introduces the proposed protocol; Section 4 reports on a performance analysis of the protocol and describes the characteristics of the security properties; Section 5 addresses a formal verification of the protocol; finally, Section 6 provides the conclusions and suggests some future work.

5.2.Related Work

Significant security concerns for the V2G connection include the guarantee of the services provider, i.e., EV privacy and its authentication in the network. EV requires the preservation of its private information from any intermediate device in the connection between EVs and the authentication provider.

Several protocols have been proposed for authenticating EVs in a V2G network. Among these protocols, Abdallah et al. [3], Saxena et al. [5], Jie et al. [12] and Liu et al. [16] focus on the possibilities EVs can play in V2G, i.e., energy consumer, energy storer, and energy provider while performing operations of charging and discharging.

Abdallah et.al [3] proposed protocols for assuring the confidentiality and integrity of exchanged information during sessions of (dis)charging. The possible situations of the EVs are defined, i.e., energy storer, when CC produces more energy than that demanded; it sends a message to the EVs of the area for them to purchase this energy and avoid energy loss; energy provider, when CC produces less energy than that demanded; it sends a message to the EVs of the area for them to sell part of their energy and avoid overcharge; energy consumer, when the EV must charge energy; and energy seller, when the EV wishes to sell unnecessary energy.

Jie et.al [12] designed an authentication protocol that preserves the privacy of user's data in the connection of their electric vehicles for the charging or discharging of batteries in the V2G network. It also optimizes communications through aggregators and dynamically manages the system. It uses group signatures and a partially blind signature restrictive technique based on identity. The architecture comprises five entities, namely Central Aggregator (CAG), LAG, Charging/discharging station (ST), Plug-in electric vehicle (PEV) and a trusted authority (TA). The protocol consists of the following four phases:

- Initial Configuration: all entities send their identities to the TA, which generates a pair of keys (public and private) for each entity and sends them to their corresponding entity. Each LAG generates a security parameter for each ST connected to it and defines functions and mathematical operations to be used and the group keys (public and private). It then defines the “Commitment” vectors and their public key and a signature.
- Generation and verification of permission: each ST generates a temporary pair of public/private keys and sends them in an encrypted message with the LAG public key to the LAG with the ST information and the temporary public key is generated. LAG checks the authenticity of both message and sender through a bilinear pairing operation. If it succeeds, ST is included in the LAG group.
- Generation of group blind certificate: each PEV calculates a random value and sends it to LAG, which builds a tree where each leaf is a PEV. It also calculates a compacted path value and a signature for each PEV. LAG sends a message to each PEV containing the compacted path and a verification value. PEVs check the message and, if the verification is successful, each PEV calculates a signature with the message received and sends it to LAG, which calculates a certificate for each PEV and sends them a message containing elements, so that they can calculate their certificate.
- Access of PEV to the V2G network through ST: PEV sends a message with its signature to ST, which checks if the signature is valid in the group. If the validation is met, ST enables PEV to connect with V2G. Finally, the information exchange between PEV and ST requires the generation of a session key in a bilinear pairing operation with their public and private keys.

Saxena et al. [13] proposed two authentication protocols for the access of EVs in the Smart Grid system for the recharge and discharge of their batteries in both residential and visiting modes, so that the following security requirements can be met: integrity of messages, confidentiality of data and users' identity, mutual authentication of the entities and resistance to attacks to the system. However, for the sake of comparisons, only the protocol for the residential mode was described. The architecture designed by Saxena et al. [13] is composed of five entities, namely EVs, Charging station (CS), LAG, Certification/Registration Authority (CA/RA) and Control Center (CC). The protocol proposed by Jie et al. [12] consists of the following four parts:

- Initial configuration, where all entities generate a pair of public and private keys;
- Registration of EVs: each EV sends information to CA/RA and returns a temporary identity to the EV.

- LAG - CA/RA communication: all LAG must have the register of the temporary identities of all EVs registered in CA/RA, therefore, the communication between LAG - CA/RA occurs for updating the register of such entities.
- Protocol execution: when an EV must charge or discharge (sell) part of its energy, it approaches a CS, establishes communication with LAG and generates a session key that guarantees a mutual authentication between EV and LAG. The EV calculates an identity verification parameter and sends an encrypted message to the LAG with the session key. The LAG decrypts the researched message, adds information for the verification of the EV identity, and sends all parameters to the CA/RA in a message encrypted with the CA / RA digital signature generated by the LAG. Finally, CA/RA checks the EV identity and returns a message of commands to the EV. The remaining messages exchanged between the EV and CA/RA are encrypted under asymmetrical encryption based on blind digital firms

5.3. System Model

Figure 5.1 shows a possible V2G network architecture, composed of EVs recharging/discharging their batteries, where:

- Electric Vehicle (EV) refers to cars, motorcycles, boats, planes and other vehicles powered by electric energy stored in batteries.
- Charge/Discharge Stations (CDS) - installed in strategic locations, that charge or discharge the electrical energy of the vehicles' batteries.
- Aggregators (AGs) are distributed in different regions of a city; a Local Aggregator (LAG) groups information from several EVs for decreasing the network communication costs; a Central Aggregator (CAG) concentrates information received from EV's;
- Authentication Server (AS) that validates the identity and credentials of EVs and stores their corresponding attributes. A distributed architecture with a Central Authentication Server (CAS) located in a control center and connected to several Substation Authentication Servers (SAS) can be used for a large system, as the SG network.
- Control Center (CC) an operations center that controls the whole electric network. The CAS that concentrates the information safely sent by SAS is installed in the CC.

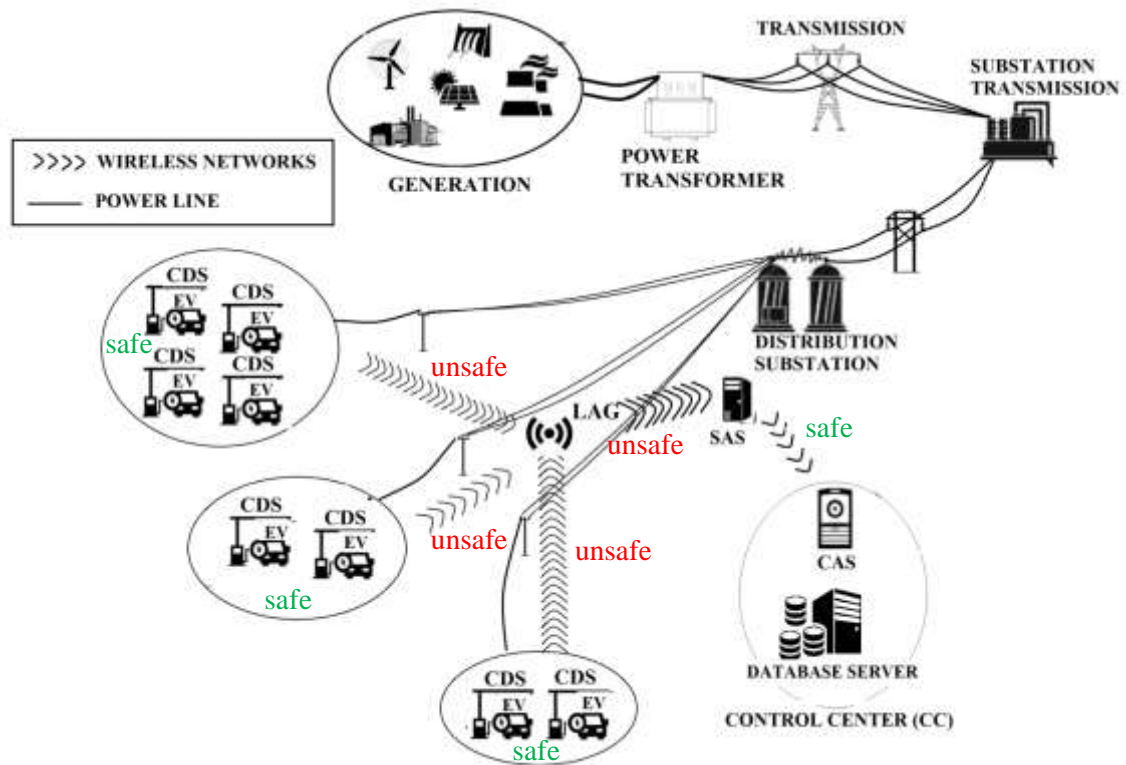


Figure 5.1- Architecture of a V2G Network

An EV can charge or discharge its battery in any CDS of the V2G network through the same protocol for both residential and visiting modes. Several CDSs can be connected to a LAG that sends information to SAS. The communications between CDSs and LAGs and between LAGs and SAS commonly occur through wireless networks.

5.4. Adversary Model

We consider the architecture presented in Figure 5.1, where the communication channels between the SAS and the CAS, between the EV and CDS and the SMS channel through which the token is sent are **safe** and efficient. The communication channels between the EVs and the LAG and the channels between the LAG and the SAS are considered **unsafe**.

There are different types of attacks that can be executed over the unsafe channels, as described below:

- An attacker may represent a valid EV so that the system charges the charged energy to a victim user, or may also turn a valid EV into an unknown EV to prevent it from recharging or discharging energy;
- An attacker may be in the path among the architecture entities proposed to perform a man-in-the-middle (MiTM) attack. This attack makes the devices believe that they are communicating between authentic entities, but it is an attacker who is sending and receiving the messages;

- An attacker can intercept messages from EVs, AG, or SAS to try to acquire information about: EV (Owner, account data), AG (Configuration and user identities), or SAS (Settings, user identities, EVs location);
- An attacker can mount DoS (Denial of Service) attacks so that users cannot reload or unload their vehicles.

5.5. Proposed Protocol

Figure 5.2 shows an overview of the operation of the proposed protocol, as follows:

1. A group of EVs located in a specific area sends a connection request of Loading / Unloading to the aggregator;
2. The aggregator groups the connection requests of the EVs and sends the connection requests in a group so that the AS validates the identities;
3. a) In case the SAS does not have a registration of the EV, it requests the CAS to authenticate the EV; in case the CAS does not have the user's information, it sends a message to the SAS to disconnect the communication with that user. b) On the other hand, if the user is authenticated, the CAS sends necessary information for the connection between EV and SAS. Once the EVs have been authenticated, the SAS sends by a secure channel a message to the EVs with the temporary identity of the group (TID_G) as calculated by the AG;
4. In addition, the SAS calculates values that will be sent by broadcast, which will allow the EVs and AG to calculate the session key and verify the authenticity of the message.

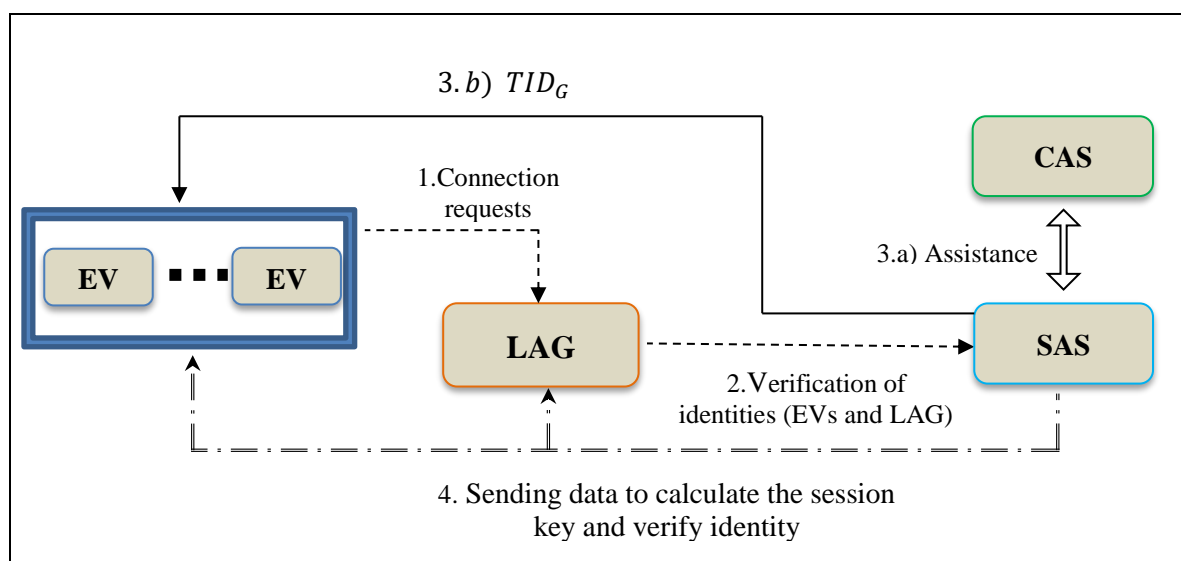


Figure 5.2- General scheme of the proposed protocol.

An adequate encryption scheme is required as part of an authentication protocol to provide security in communications. In this sense, the proposed protocol aggregates group devices to provide simultaneous authentication using an encryption method that combines Identity-Based Signcryption (IBSC) with bilinear pairing ([17], [18]). Bilinear pairing was used to generate the session key and verify whether the message received by EVs had been sent by the correct entity.

The proposed protocol has 3 phases, shown in figure 5.3:

- Initialization, where the mathematical elements and entities to be used are defined;
- Registration, where all entities of the network associate their characteristic data to a certificate and the public key to be identified;
- Authentication, where some entities not connected to the network try to demonstrate they are a legitimate part of it and, once correctly identified, proceed to use their services through a session. When the use of the service is finished, the session is completed and the entity is disconnected from the network.

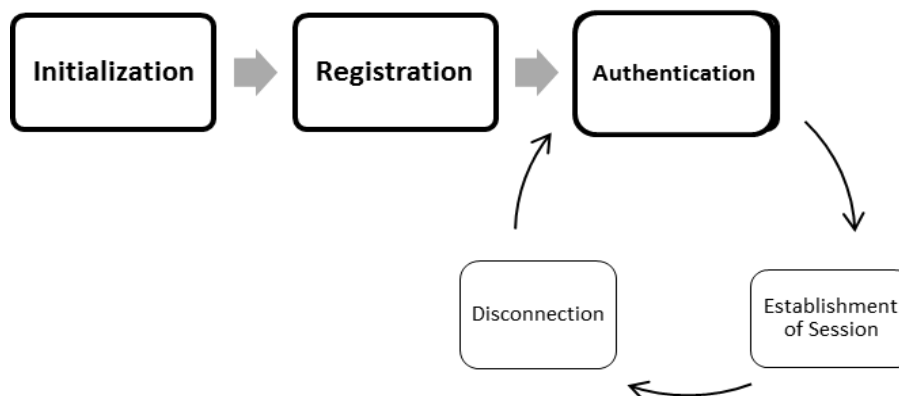


Figure 5.3- Phases of the Proposed Protocol

The phases of the protocol are described in detail below. The dotted arrows represent the sending of messages through unsafe channels and continuous arrows represent the sending of messages through secure channels.

1st. phase: **Initialization of the system**

Two cyclic groups G and G_T of order q and P , and a generator element of group G are chosen. G and G_T are supposedly related to a non-degenerative pairing and a bilinear map that can be efficiently computed:

$\hat{e} : G \times G \rightarrow G_T$ such that $\hat{e}(P, P) \neq 1_{G_T}$ and $\hat{e}(aP_1, bQ_1) = \hat{e}(bP_1, aQ_1) = \hat{e}(P_1, Q_1)^{ab} \in G_T$ for every $a, b \in \mathbb{Z}_q^*$ and every $P_1, Q_1 \in G$. Moreover, the *hash* functions of the system are defined: $H_1: \{0,1\}^* \rightarrow G$, $H_2: \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and $H_3: G \rightarrow \mathbb{Z}_q^*$.

Finally, the central authentication server (AS) and all aggregators (AG) define an elliptical curve on a finite field $E(F_q)$ and parameters $\{G, G_T, \hat{e}, P, H_1, H_2, H_3\}$ are published.

AS then chooses a private key $x_{AS} \in \mathbb{Z}_q^*$ and calculates its public key $Y_{AS} = x_{AS} * P$ to be published.

2nd. phase: Registration of Electric Vehicles and Aggregators

All EVs and AGs must register on-site in the energy supplier's system. The registration of an EV is initialized when it chooses an ID_{EV} identity and an $x_{EV} \in Z_q^*$ private key. It then calculates $y_{EV} = x_{EV} * P$ public key. The user sends a message containing the public key and the user's identity $\{y_{EV}, ID_{EV}\}$ to AS through a secure channel. AS saves the data received, i.e., y_{EV} and ID_{EV} and associates the EV attributes, as model, make, owner, chassis number and telephone numbers related to the vehicle. It then calculates the vehicle's certificate $Cert_{EV} = H_1(ID_{EV} || model || make || chassis\ number) * x_{AS}$ and sends a message containing the certificate and the hash value of its identity $\{Cert_{EV}, h_{EV}\}$.

An identity (ID_{AG}) must be chosen for the registration of AGs. The aggregator then chooses a random number $x_{AG} \in Z_q^*$ to be its private key and calculates a public key $y_{AG} = x_{AG} * P$. AG sends AS a message containing the public key and the identity of the device $\{y_{AG}, ID_{AG}\}$. AS stores the data received y_{AG} and ID_{AG} and calculates $P_{AG} = H_1(y_{AS}, y_{AG}, LAI)$, where LAI (local area identifier) identifies the area where the aggregator is located. The certificate is then calculated $Cert_{AG} = x_{AS} * P_{AG}$ and AS sends AG a message $\{Cert_{AG}, P_{AG}\}$ to be stored in the device. Certificate $Cert_{AG}$ is published in the network. Figure 5.4 summarizes the registration phase.

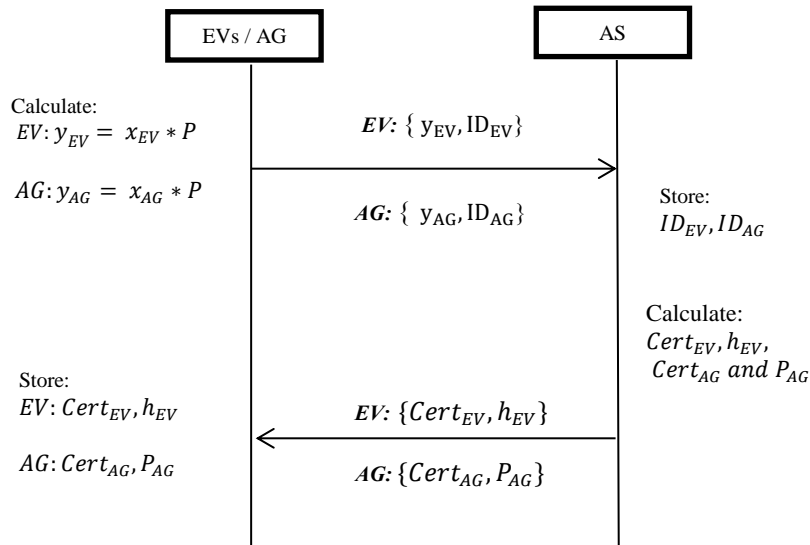


Figure 5.4- Registration Phase

3rd. phase: Authentication of EV and AG

In the authentication phase, the proposed protocol exchanges four messages:

$$1) \quad \text{EV} \{ S_{i-j}, M_{EV_{i-j}}, MAC_{i-j} \} \text{AG} \rightarrow$$

EV_j chooses a random number $v_{EV_{i-j}} \in Z_q^*$ and calculates the following values:

$$A_{i-j} = v_{EV_{i-j}} * P$$

$$S_{EV_{i-j}} = (y_{AG_i} * x_{EV_j})$$

$$M_{EV_{i-j}} = (A_{i-j} || Cert_{EV_i})$$

$$MAC_{EV_{i-j}} = h_2(M_{EV_{i-j}} || S_{EV_{i-j}})$$

where $S_{EV_{i-j}}$ is the challenge for the aggregator to guarantee the identity of V_{i-j} .

Message $\{M_{EV_{i-j}}, S_{EV_{i-j}}, MAC_{EV_{i-j}}\}$ is sent to AG_i .

$$2) \quad \underline{\underline{AG}} \quad \underline{\underline{\{S_{AG_i}, M_{G_i}, MAC_{G_i}\}}} \quad \underline{\underline{AS}} \quad \rightarrow$$

AG_i searches for public key y_{EV_j} associated with $Cert_{EV_j}$ and checks identity $S_{EV_{i-j}} = S'_{EV_{i-j}} = (y_{EV_{i-j}} * x_{AG_i})$. If it succeeds, it calculates and checks the authentication code of the message: $MAC_{EV_{i-j}} = MAC'_{EV_{i-j}} = h_2(M_{EV_{i-j}} || S'_{EV_{i-j}})$. If the comparison is satisfactory, AG_i adds message $M_{EV_{i-j}}$ to a group message $M_{G_i} = (M_{EV_{i-1}} || M_{EV_{i-2}} || \dots || M_{EV_{i-j}} || \dots || M_{EV_{i-n}})$. Otherwise, if no comparison is satisfactory, the connection with EV is terminated.

At the end, the aggregator chooses two values $v_{G_i}, v_{AG_i}, TID_{G_i} \in Z_q^*$, calculates

$$TID_{G_i} = H_1(ID_{AG_i}) * v_{G_i}$$

$$A_i = v_{AG_i} * P$$

$$S_{AG_i} = (y_{AS_i} * x_{AG_i})$$

$$M_{AG_i} = (A_i || Cert_{AG_i} || TID_{G_i})$$

$$MAC_{AG_i} = h_2(M_{EV_{i-j}} || S_{EV_{i-j}})$$

where TID_{G_i} is the group identifier, and adds its message M_{AG_i} to group $M_{G_i} = \{M_{EV_{i-1}} || M_{EV_{i-2}} || \dots || M_{EV_{i-j}} || \dots || M_{EV_{i-n}} || M_{AG_i} || v_{G_i}\}$. It then performs

$$MAC_{G_i} = (MAC_{AG_i} \oplus MAC_{EV_{i-1}} \oplus MAC_{EV_{i-2}} \oplus \dots \oplus MAC_{EV_{i-j}})$$

to calculate the authentication message of group MAC_G .

Message group M_{G_i} , MAC_{G_i} and challenge S_{AG_i} are immediately sent to AS.

$$3) \quad \leftarrow \underline{\underline{AG}} \quad \underline{\underline{\{\varphi, X_1, X_2, t_4\}}} \quad \underline{\underline{AS}}$$

AS checks the identity of the aggregator calculating challenge $S_{AG_i} = (y_{AG_i} * x_{AS})$ and compares $S_{AG_i} = S'_{AG_i}$. If the calculation fails, AS sends an error message to the group and terminates the authentication process. Otherwise, it calculates MAC'_{AG_i} and all $MAC'_{EV_{i-j}}$ and the total MAC of the message.

$$MAC'_{G_i} = (MAC'_{AG_i} \oplus MAC'_{EV_{i-1}} \oplus MAC'_{EV_{i-2}} \oplus \dots \oplus MAC'_{EV_{i-j}})$$

For checking the integrity of all messages with the following comparison: $MAC_{N_i} = MAC'_{N_i}$. If the verification fails, AS sends a MAC failure message to the group. Otherwise, it chooses a random number $v_{AS1}, v_{AS2}, r \in Z_p^*$ and calculates a temporary identity and a temporary key for the group.

$$TID_{G_i} = H_1(ID_{AG_i}) * v_{G_i}$$

$$TN_i = h_2(TID_{G_i} || v_{AS1})$$

AS then sends an SMS to the EVs of the group with the temporal identity of the group TID_{G_i} , and calculates the values shown in Table 5.1.

Table 5.1- Calculation of Values for a Broadcast message.

$F = v_{AS2} * TN_i * Y_{AS}$	$Cert_{G_i} = x_{AS} * TN_i$
$X_1 = r * TN_i$	$X_2 = r * y_{AS}$
$w_1 = r * H_1(TID_{G_i}) * y_{AS}$	$h = H_1(X_1 X_2 TN_i)$
$z = H_2(h + Cert_{G_i} + w_1)$	$w_2 = r * Cert_{AG_i} * TN_i$
$\varphi = H_2(w_1 w_2) \oplus (z Cert_{G_i} v_{AS1} F)$	

AS sends a broadcast message $\{\varphi, X_1, X_2, t_4\}$, where t_4 is a *timestamp*, to all group members and calculates the session keys and the hash of each EV_{i-j} and AG_i . The operations are shown in Table 5.2.

Table 5.2- Calculation of the SAS session Keys.

EV_{i-j}	AG_i
$KS'_{i-j} = \hat{e}(A_{i-j}, F) \hat{e}(x_{AS}, v_{sp2} * TN_i * Y_{EV_{i-j}})$	$KS'_i = \hat{e}(A_i, F) \hat{e}(x_{AS}, v_{sp2} * TN_i * Y_{AG_i})$
$Hks_{i-j} = H_4(KS_{i-j})$	$Hks_i = H_4(KS_i)$
$Mk_{i-j} = (Hks_{i-j} Cert_{EV_{i-j}})$	$Mk_i = (Hks_i Cert_{AG_i})$

4) **EV/AG** $\{Mk_{i-j}\}\{Mk_{i-j}\}$ **AS**
 ----- ➔

When EVs and AG_i receive the message from AS , they calculate the following values: $w'_1 = H_1(TID_{G_i}) * X_2$; $w'_2 = X_1 * Cert_{AG}$, where $Cert_{AG}$ is an aggregator certificate published on the network. Then the EVs and the GA perform an **xor** operation to extract the parameters to calculate the session key and check the message sent by AS .

$$\varphi \oplus H_2(w'_1 || w'_2) = (z || Cert_{G_i} || v_{AS1} || F).$$

With $z, Cert_{AG}, v_{AS1}$ and F values found in the message, EV and AG do the following actions:

- Verification of the message:

To check the message sent by AS, the EVs and the AG must calculate $TN'_i = H_2(TID_{G_i} || v_{AS1})$ and $h = H_1(X_1 || X_2 || TN_i)$, where X_1 and X_2 are the values received in the message and TN_i is the group key found in the message. EV must then verify $z' = H_2(h' + Cert'_{G_i} + w'_1)$.

If the verification succeeds, EV_s and AG_i calculate the session key; otherwise, they close communication.

- Session key

The EVs and the AG must use the following elements to calculate the session key:

- Private Keys
- Random values generated
- Value obtained from the message sent by AS (v_{AS1})
- Identification value of the group (TID_{G_i})

Once the session key is generated, the EVs and AG calculate a hash of that key and form a message that contains the entity certificate (EVs or AG) and the session key hash. This message is encrypted by an xor operation with the group key. The operations described above are shown in Table 5.3:

Table 5.3- Calculation of EVs and AG session keys.

EV_{i-j}	AG_i
$F = H_2(TID_{G_i} v_{AS1})$	
$KS_{i-j} = \hat{e}\left(\left(A_{i-j} + x_{EV_{i-j}}\right), F\right)$	$KS_i = \hat{e}\left(\left(A_i + x_{AG_i}\right), F\right)$
$Hks_{i-j} = H_4(KS_{i-j})$	$Hks_i = H_4(KS_i)$
$Mk_{i-j} = (Hks_{i-j} Cert_{EV_{i-j}}) \oplus TN_i$	$Mk_i = (Hks_i Cert_{AG_i}) \oplus TN_i$

The encrypted messages of EV ($\{Mk_{i-j}\}$) and AG $\{Mk_i\}$ are sent to the AS for verification.

AS immediately receives the messages from each EV_{i-j} and AG_i , groups them and calculates their MAC'_{Mk_i} , groups them and calculates MAC_{Mk_i} of the keys and certificates calculated by AS:

$$MAC_{Mk_i} = H_2((Hks'_i || Hks'_{i-1} || Hks'_{i-2} || \dots || Mks'_{i-j}) \oplus TN_i)$$

$$MAC'_{Mk_i} = H_2((Hks'_i || Hks'_{i-1} || Hks'_{i-2} || \dots || Mks'_{i-j}) \oplus TN_i)$$

If $MAC'_{Mk_i} = MAC_{Mk_i}$ are the same, all group members have the correct session key, therefore, communication is established. On the other hand, if the verification fails, AS checks, one by one, the **Hash** of the keys sent. When it finds the wrong key, it closes communication with this member and creates a new temporary group key, which is sent to each member in an encrypted mode with the session key established.

Below is the mathematical proof of the establishment of the session keys.

$$\begin{aligned}
KS_{i-j} &= \hat{e}\left((A_{i-j} + x_{EV}), F\right) \\
&= \hat{e}(A_{i-j}, F) \hat{e}\left(x_{EV_{i-j}}, v_{sp2} * TN_i * Y_{AS}\right) \\
&= \hat{e}(A_{i-j}, F) \hat{e}\left(x_{EV_{i-j}}, v_{sp2} * TN_i * x_{AS} * P\right) \\
&= \hat{e}(A_{i-j}, F) \hat{e}\left(x_{AS}, v_{sp2} * TN_i * x_{EV_{i-j}} * P\right) \\
&= \hat{e}(A_{i-j}, F) \hat{e}\left(x_{AS}, v_{sp2} * TN_i * Y_{EV_{i-j}}\right)
\end{aligned}$$

Figure 5.5 shows the flow of messages exchanged among the entities.

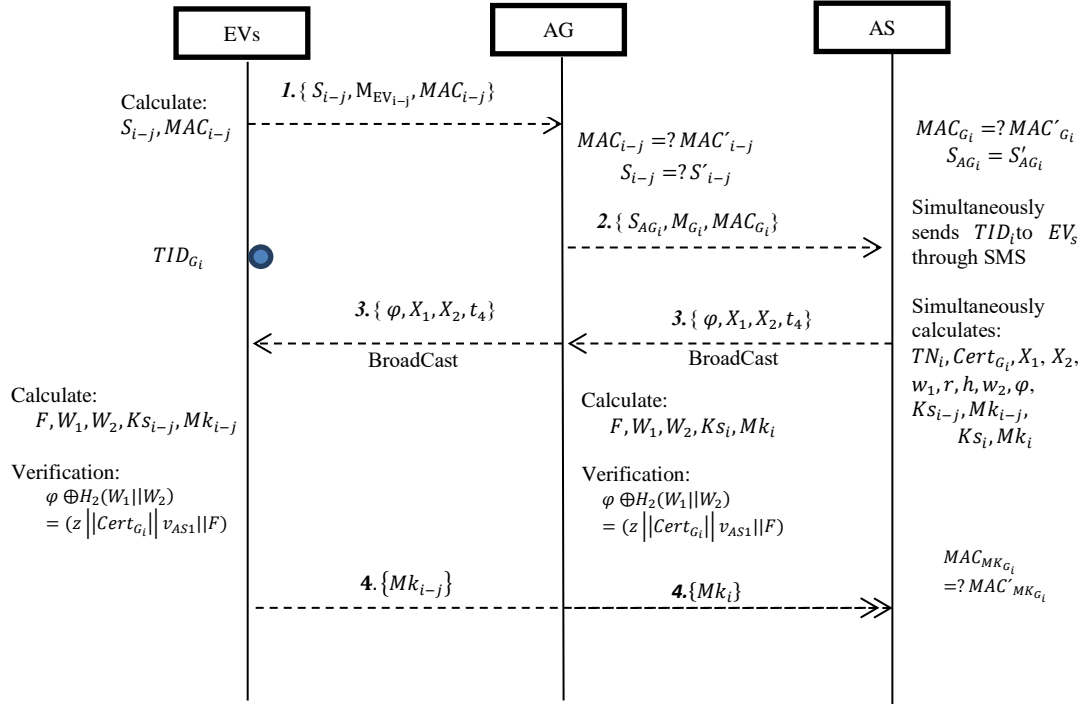


Figure 5.5- Authentication phase.

An EV can charge or discharge its battery in any CDS of the V2G network using the same protocol for the residential and visiting modes. Several CDSs can be connected to a LAG that sends information to ASs. Communications between CDSs and LAGs and between LAGs and SAS are established through wireless networks. The proposed protocol can support authentication in both modes, i.e., residential and visiting, once the hierarchic distribution of AS enables the authentication of EVs anywhere. It also can operate in different situations/cases, such as storer, provider, consumer and seller, where the interaction of an EV in the connection with V2G occurs as described below:

- Energy Storer: when CC detects power plants are producing more energy than that demanded in a certain area, it sends a broadcast message to the EVs group through AS and LAG of the area for them to purchase such energy for the avoidance of loss. If an EV wishes to purchase the energy, it must only respond to AS with a message containing the EV temporal identity encrypted with the group key. The remaining communication will be established with the session key of each EV;

- Energy Provider: when CC detects power plants are producing less energy than that demanded in a certain area, it sends a broadcast message to the group of EVs through AS and LAG of the area for them to sell part of their energy for the avoidance of overcharge in the power plant. If an EV wishes to sell energy, it must only respond to AS with a message containing the EV temporal identity encrypted with the group key. The remaining communication will be established with the session key of each EV;
- Energy Consumer or Seller: when EV approaches an EDC to charge or discharge its battery, an encrypted communication is established with CC through a session key employing AS.

Below is a comparative table of the entities that compose the V2G architecture of the above-mentioned studies and the protocol proposed.

Table 5.4 shows the difference among the entities of the architecture proposed in this chapter and those proposed by Saxena et al. [13] and Jie et al. [12]. According to those authors, aggregators perform most tasks of verification of messages and authentication of EVs, consequently, LAG must show high processing power for avoiding overcharge. Conversely, as the authentication server of the proposed protocol shows high processing power, it uses the aggregator only for grouping messages and reducing communication costs, which results in a more flexible V2G network.

Table 5.4- Comparisons of entities of the V2G architecture

Entities	Jie et al. [12]	Saxena et al. [13]	Proposed protocol
<i>EV</i>	✓	✓	✓
<i>ST/CE/CDS</i>	✓	✓	✓
<i>LAG</i>	✓	✓	✓
<i>CAG</i>	✓	--	--
<i>SAS</i>	--	--	✓
<i>CAS</i>	--	--	✓
<i>TA/TTP/CA/RA</i>	✓	✓	--
<i>CC</i>	--	✓	✓
Total Number of Entities	5 Entities	5 Entities	6 Entities

5.6. Security and Performance Analyses

This section reports on an analysis of the security and performance of the proposed protocol and a comparison with the other protocols used for authentication of a V2G system.

5.6.1. Security Analysis

Below is a description of the processes related to authentication, preservation of privacy and integrity and analytical evaluation of the resistance of the proposed protocol to attacks.

1) Mutual Authentication: Mutual Authentication is established among EVs , AG and AS . AG authenticates EVs verifying challenge $S_{EV_{i-j}}$. AS authenticates AG through challenge S_{AG_i} . EVs authenticate AG and AS by means of *token* TID_i in the calculation phase of the group's temporal key through a pairing operation of the message sent by AS .

2) Preservation of privacy: The identity of the EV is kept confidential by the authentication servers; the other entities of the V2G network know only the temporary identity and the EV certificate.

3) Protection to integrity: The integrity of the messages exchanged is maintained with the MAC generation. An adversary cannot make changes to an intercepted message without the MAC value changing, so the system would identify if a message was manipulated.

4) Prevention against attacks: we will describe the different types of attacks that can affect the V2G network and how the proposed protocol can resist them:

- Personification: an attacker that aims at impersonating a valid EV must know its the identity and secret key. However, parameter $S_{EV_{i-j}}$ or S_{AG_i} cannot be obtained without the secret keys of the involved entities. A session key is generated whenever an EV_s is authenticated for the avoidance of use of old parameters in other devices.
- MITM: after receiving a message from AG , AS sends to EVs an OTP through another channel to check the identity of EVs towards protecting the system from such an attack. EV_s must perform operations with both the values contained in the message received and the OTP (TID_i) sent by the server for obtaining the session key and validating the identity of AG_{AG_i} and AS .
- Repetition and Injection: an attacker can intercept a message to carry out a repetition attack and inject data in the message. Therefore, random numbers chosen for each session, as A, v, TID_i, ks are implemented and *hash* functions check the integrity of the message.
- -Redirectioning: whenever a new EV tries to access the system, it is associated with a group attended by an AG_i . If the same user tries a second access to either the same group, or a different one, AS rejects the second connection.
- Known key: the proposed protocol generates and sends an OTP (TID_i) to the EV to calculate a key for each session, so that an attacker cannot use old keys or data to establish a communication.
- DoS: The Server will enable a valid EV to access the V2G network by calculating the $S_{EV_{i-j}}$ challenge. If more than one session is requested, the server checks the location of the request and if differences between AG_i of the requests sent by the same user are detected, the system rejects the communication of this user to avoid even DDoS attacks

5.6.2. Formal Verification of the Proposed Protocol.

This section discusses the formal verification of the proposed protocol, introduces codes that represent the protocol in a high level language and provides the results of a simulation with AVISPA tool [20].

AVISPA is a formal verification tool vastly used for internet security assessment. It uses the HLPSL language that enables the description of entities, as well as exchange of messages necessary for the operation of the protocol.

The tool has four back-ends, among which we use On-the-Fly Model Checker (OFMC) and the Constraint-based Attack Finder (CL-AtSe). The verification of results is simple, i.e., "SAFE" is shown if no problem has been detected, and "UNSAFE" is shown otherwise. It is then possible to verify the security properties as well as vulnerability to various types of attacks [20].

5.6.2.1. Modeling of the Proposed Protocol in HLSPL

HLPSL allows the construction of protocol models that requires the specification of the sequence of actions of each type of protocol participant in a module. Part of the HLSPL codes is shown in Figures 5.6, 5.7 and 5.8 to illustrate how the proposed protocol was modeled for the simulation of its behavior and validation of security in the AVISPA tool.

Figure 5.6 shows the HLSPL code that models the developed behavior or role of one of the entities considered in the protocol. The structure of the HLSPL code of the EV role is the same of those of the codes of the other entities (AG and AS) and consists of the following parts:

- Statement of the agents, communication channels and constants known by the entity.
- Declaration of variables calculated or received by other entities.
- Statement of the functions to be used.

Once the above-mentioned statements have been made, the states are created. Such states describe the operations and messages to be exchanged with the other entities and are differentiated by a number assignment. At the end of each State, the elements that must be kept secret are declared.

```

role role_EV(EV,AG,AS:agent,P,Xev,Yij,Yag,Yas,Certev,Certg,Certag:text,SND1,RCV1:channel(dy))

played_by EV
def=
  local
    State:nat,
    Sev,T1,G,X1,X2,T4,W1,W2,Z,Vev,Vas1,F,TNi,Mev,MACev,Aij,Mij,V,Mkij,Hkij,TIDg:text,
    Kij:symmetric_key,
    MAC,H1,H2,M,E,Sum:function

  init
    State := 0
  tRansition
    1. State = 0 ∧ RCV1(staRt) => State' := 1 ∧ SND1(Mev',Sev',MACev') ∧ Vev' := new()
    ∧ Aij' := M(Vev',P) ∧ Mij' := (Aij'.Certev') ∧ Sev' := M(Yag,Xev) ∧ MACev' := H1(Sev'.Mij')

    4. State = 2 ∧ RCV1(G'.X1'.X2'.T4') => State' := 3 ∧ TNi' := H2(TIDg',Vas1)
    ∧ W1' := M(H1(TIDg'),X2) ∧ W2' := M(Certag',X1') ∧ V' := xor(G',H2(W1'.W2'))
    %∧ J' := V'.Z'.Certg'.Vas'.F' ∧ F' := H2(TIDg',Vas1) ∧ Kij' := E(Sum(Aij',Xev),F)
    ∧ Hkij' := H1(Kij') ∧ Mkij' := xor((Hkij'.Certev'),TNi')
    ∧ SND1(Mkij') ∧ secret(TNi',sec_1,{}) ∧ secret(Kij',sec_2,{AS,EV})

  end role

```

Figure 5.6- Role of EV in HLSPL

Figure 5.7 shows (in HLSPL language) a role session that describes how a session is established and the role environment that describes the environment where the protocol is executed. The elements (variants, keys, agents, etc.) of the protocol an attacker can somehow acquire are also declared.

```

role session(EV,AG,AS:agent,
  P,Xev,Yev,Yag,Yas,Certev,Certg,IDag,Certag,Xag,Xas,Aij,Ai:text,
  SND1,RCV1:channel(dy))
def=
  composition
    role_EV(EV,AG,AS,P,Xev,Yev,Yag,Yas,Certev,Certg,Certag,SND1,RCV1)
    ^ role_AG(EV,AG,AS,P,IDag,Certev,Yas,Xag,Yev,SND1,RCV1)
    ^ role_AS(EV,AG,AS,P,Yag,Yev,IDag,Yas,Xas,Certev,Certg,Certag,SND1,RCV1)
  end role

role environment()
def=
  const
    p,xev,yev,yag,yas,certev,certg,idag,certag,xag,xas,aij,ai:text,
    ev,ag,as:agent,
    sec_1,sec_2,sec_3,sec_4,sec_5,sec_6:protocol_id,
    snd1,rcv1:channel(dy)

    intruder_knowledge = {ev,ag,as,p,certev,certg,certag,aij,ai}

  composition
    session(ev,ag,as,p,xev,yev,yag,yas,certev,certg,idag,certag,xag,xas,aij,ai,snd1,rcv1)
    ^session(i,ag,as,p,xev,yev,yag,yas,certev,certg,idag,certag,xag,xas,aij,ai,snd1,rcv1)
    ^session(ev,i,as,p,xev,yev,yag,yas,certev,certg,idag,certag,xag,xas,aij,ai,snd1,rcv1)
    ^session(ev,ag,i,p,xev,yev,yag,yas,certev,certg,idag,certag,xag,xas,aij,ai,snd1,rcv1)
  end role

```

Figure 5.7- Specification of the role of session in HLSPL

Finally, Figure 5.8 shows the security objectives that the protocol must guarantee, considering the definition of elements declared as secret in the roles of the entities; the values that were considered as security objectives in the protocol proposed are described below:

secrecy_of sec_1: represents the session key K_{ij} , which in the end can only be known by the EV and the SAS.

secrecy_of sec_2: represents the identity of the EV (ID_{EV}), which can only be ascertained by the EV and SAS.

secrecy_of sec_3 : represents the group verification message M_k that can only be known by the authentic entities EV, AG and SAS.

secrecy_of sec_4: represents the session key SK_i , which in the end can only be known by the AG and the SAS.

secrecy_of sec_5: represents the identity of the AG (ID_{AG}), which can only be ascertained by the AG and SAS.

secrecy_of sec_6: represents the Temporal Identification group TN_i , which in the end can only be known by the EV, AG and the SAS.

```

goal
  secrecy_of sec_1
  secrecy_of sec_2
  secrecy_of sec_3
  secrecy_of sec_4
  secrecy_of sec_5
  secrecy_of sec_6

end goal

environment()

```

Figure 5.8- Security objectives and related secrets of the proposed protocol in HLSPL

5.6.2.2. Security Check Results

Simulations performed with the OFMC and CL-AtSe back ends verified the protocol security. If the simulated protocol shows security problems, AVISPA provides a detailed result of the successful attack, whereas if the protocol is safe, AVISPA shows summarized information of the simulation. If the simulation results show the protocol is safe for both back-ends, with the results shown in figure 5.9

<pre> % OFMC % Version of 2006/02/13 SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS PROTOCOL /home/span/span/testsuite/results/artigo_3v_3.if GOAL as_specified BACKEND OFMC COMMENTS STATISTICS parseTime: 0.00s searchTime: 0.24s visitedNodes: 27 nodes depth: 3 plies </pre>	<pre> SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS TYPED_MODEL PROTOCOL /home/span/span/testsuite/results/artigo_3v_3.if GOAL As Specified BACKEND CL-AtSe STATISTICS Analysed : 15 states Reachable : 15 states Translation: 0.08 seconds Computation: 0.01 seconds </pre>
---	--

Figure 5.9- Security Simulation Results for OFMC and CL-AtSe

The results of the simulation of the HLSPL code of the proposed protocol applying the backend of the OFMC are shown in Figure 5.9 (a). In the summary part indicates that the protocol is secure. In the statistics part you can see that the search time was 0.07 seconds, the number of visited nodes was 27 and the depth was 3.

The Figure 5.9 (b) shows the results of the execution of the proposed HLSPL code on the back-end CL-AtSe. In the summary it is concluded that the protocol is secure. In the statistics you can see that 15 states were analyzed, 15 states were reached, the translation took 0.08 seconds and the computation was 0.01 seconds.

5.6.3. Simulation of intrusion with SPAN

The interaction of the entities of the proposed protocol can be seen in the security protocol Animator (SPAN) depleted by the researchers of AVISPA Tools. Figure 5.10 shows the simulation of an invader between EV and AG and Figure 5.11 shows the simulation of the proposed protocol interacting with an intruder between the AG and the SAS.

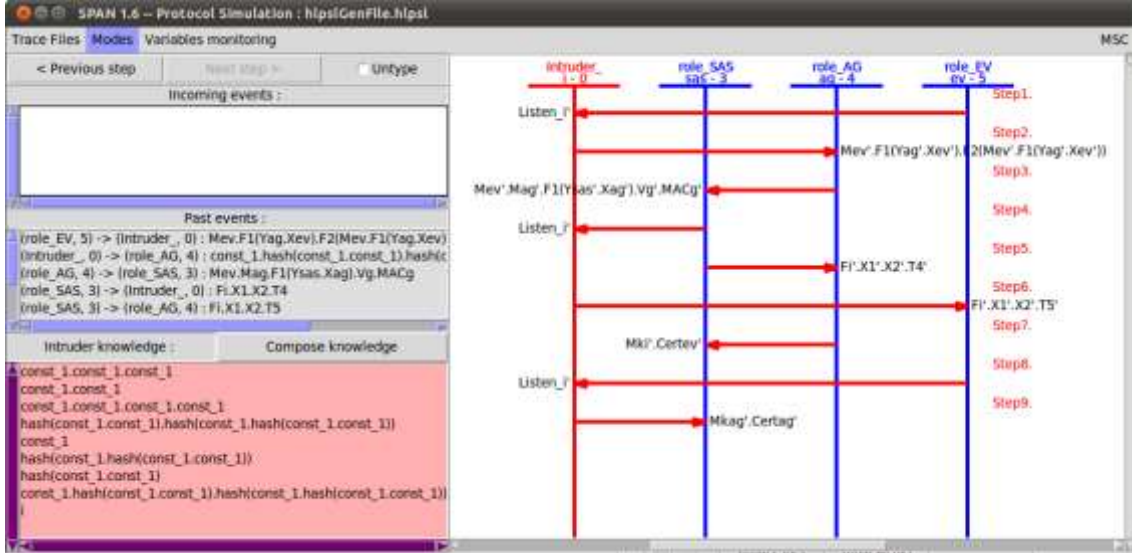


Figure 5.10 Intrusion simulation between EV and AG with SPAN

From the simulation of Figure 5.10, we can analyze the behavior of the proposed protocol before an attacker located between the EV and the AG.

i. Impersonation Attack:

An attacker may execute a proxy attack between the EV and the AG. The attacker can execute a proxy attack in two scenarios:

Scenario 1: An attacker can try to represent a valid EV and change the challenge $S_{EV_{i-j}}$, but AG will check the integrity of the message with the MAC_{EV} of the message, think it was modified and terminate the connection.

Scenario 2: An attacker can change the $S_{EV_{i-j}}$ and the MAC_{EV} of the message and send the message to the AG, but the attacker cannot generate a challenge $S_{EV_{i-j}}$ valid than $Cert_{EV_i}$ because it does not know the private key x_{EV_j} of the EV, so the AG identifies this EV as invalid and would terminate communication with it.

ii. MITM attack:

An attacker can intercept messages exchanged between the EV and the AG to steal information and gain access to the system. In figure 5.10 an attacker who establishes a communication with the EV and another with the AG. The MiTM attack can be performed in three scenarios:

Scenario 1: An attacker can attempt to change $M_{EV_{i-j}}$, but since it can not generate an $S_{EV_{i-j}}$, then when AG checks the challenge, that the message is not a false EV and the connection is terminated.

Scenario 2: in case the attacker only stores the EV information and forwards the authentic EV message to the AG. It will receive message-3 with the information for the session key generation, but could not generate the session key because it needs the TID_{G_i} sent the authentic EV through a secure channel and private key of the $x_{EV_{i-j}}$.

Scenario 3: An attacker may attempt to send a 3-message to the EV, but when the EV verifies the authenticity of the message, it will find that it is false and terminate the communication.

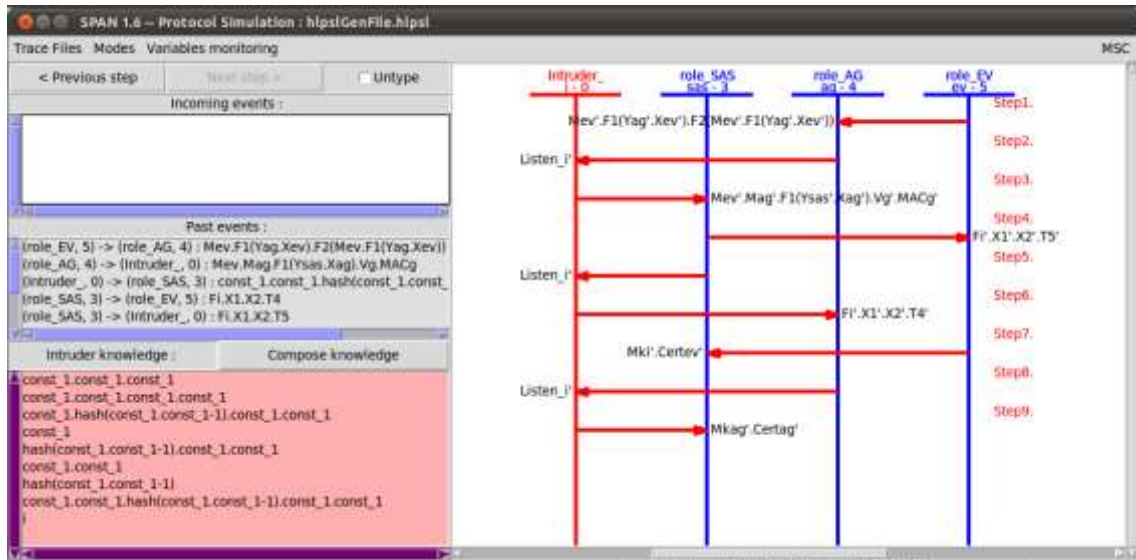


Figure 5.11- Intrusion simulation between AG and SAS with SPAN

Figure 5.11 shows the simulation of the proposed protocol with an attacker between the AG and the SAS. In this case, the behavior of the proposed protocol can be analyzed against the following attacks:

i. Impersonation Attack:

In this attack an attacker may try to pass through a valid aggregator. There are scenarios where a personification attack can be performed.

Scenario 1: An attacker may try to represent a valid AG and change the challenge S_{AG_i} , but SAS will check the integrity of the message with the MAC_{AG} of the message, think it has been modified and terminate the connection.

Scenario 2: An attacker can change the challenge S_{AG_i} , the MAC_{AG} of the AG data and the MAC_{G_i} of the group data, this message sent by the attacker to the SAS. SAS will perform an operation with its private key to verify the challenge and look for the corresponding user data, but taking into account that the attacker cannot generate a true temporary identity the authentication request will be rejected.

ii. MiTM Attack:

Messages exchanged between AG and SAS may be intercepted by an attacker to subtract information to access the system or obtain EV data. The attack has two scenarios:

Scenario 1: The attacker attempts to extract information from message-3, but cannot decipher the message because it cannot generate the values to do the right operations. In addition, to generate a valid session key you must have the AG private key.

Scenario 2: The attacker attempts to extract information from message-4, but cannot decipher the message because it does not have the required data (TN_i). In addition, the message only has the Hks_i hash of the session key and the AG certificate $Cert_{AG_i}$, this information does not break the privacy of the system data.

5.6.4. Performance Analysis

This subsection addresses an analytical evaluation of the communication and computational costs of the proposed protocol and a comparison with the other protocols cited.

a) Communication Cost

Communication cost refers to the total number of bits transmitted by a network during the execution of the protocol. The same table of values from Saxena et al.[13], showed in Table 5.5, was used for simplifying the calculations and providing an adequate comparison with other protocols.

Table 5.5- Symbols and Cost in bits [13].

Symbol	Description	Length (bits)
Name	User's name	128
ID	User's identification	128
PID	Pseudo-identity	128
$H()$	Hash function	64
x	Private key	128
y	Public key	128
k	Session key	128
Role	User's role	64
L	Location of the EV	32
T	Token	3
t	Timestamp	64
*	Multiplication operator	-
\hat{e}	Bilinear Pairing	-
SAS	Authentication Server of the substation	-
CAS	Authentication Server of the Control Center	-
Cert	Digital Certificate	128
P	Point of the elliptical curve	128
\oplus	XOR operator	-

Table 5.6 shows a comparison of the communication costs by entities for a group of n EVs connected to an AG. Such costs were measured in bits using Table 5.7.

Table 5.6- Communication cost in bits per message

	M1	M2	M3	M4	M5	M6	M7	M8	TOTAL
Jie et al. [12]	257n	64n	128n	256n	128n	128n	128n	192n	1281n
Saxena et al. [13]	384n	704n	320n	128n+320	-	-	-	-	1536n+320
Proposed Protocol	384n	256n+448	704	192n+192	-	-	-	-	832n + 1344

The total communication cost of the proposed protocol is $832(n) + 1344$ bits for n EVs per aggregator.

According to Table 6, our protocol shows better communications performance than the protocol proposed by Jie et al. [12] for a number of EVs higher than 1.45, i.e., for a number of EVs higher than or equal to 2 and better performance than the protocol proposed by Saxena et al. [13] for a number of EVs higher than or equal to 2.99, i.e., approximately 3.

Fig. 5.12 shows graphs of the communication costs of the proposed protocol and the protocols proposed by Jie et al. [12] and Saxena et al. [13]. The communication costs of all protocols increase linearly according to the number of EVs. The superior performance of our protocol in aggregators with medium or high number of EVs is clearly demonstrated.

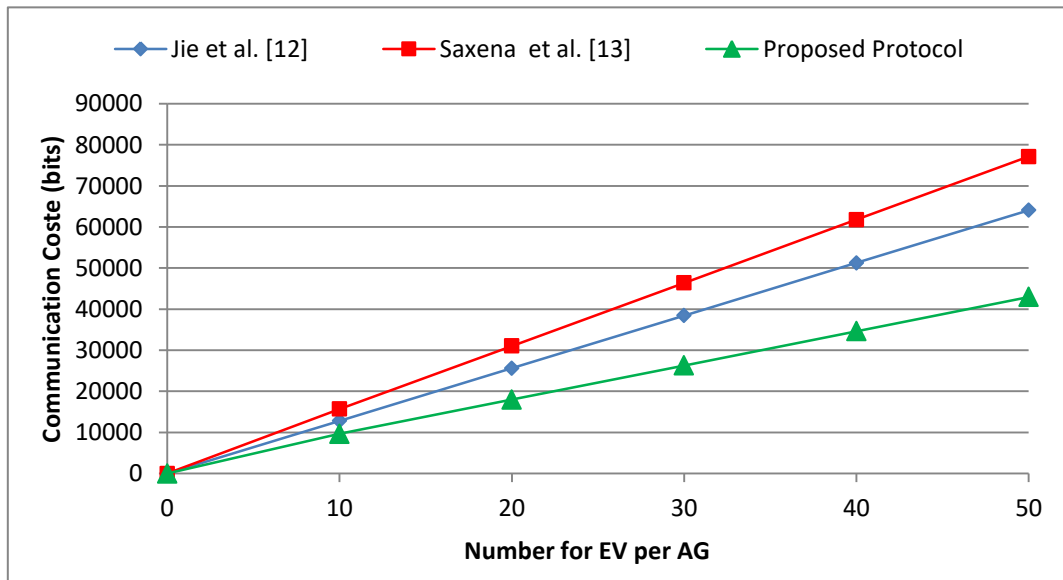


Figure 5.12- Communication Costs of the Protocols

b) Computational Cost

Here it is made is a comparison of the computational costs of our protocol and the protocols proposed by Jie et al. [12] and Saxena et al. [13]. The run-time values of the Multiplication (T_{mul}), Exponentiation (T_{exp}) and Bilinear Pairing (T_{pair}) functions are based on the values of Tao et al. [19], shown in Table 5.7, and processing parameters of involved entities.

The time costs of operations, such as hash functions, symmetric encryption / decryption, XOR, Message Authentication Code (MAC), and addition, will be omitted because their execution times are very short [19].

Table 5.7- Cost in ms of each operation and entity considered [19].

Entity	Performance parameters of involved entities			costs (ms)		
	CPU(GHz)	RAM	OS	T_{mul}	T_{exp}	T_{pair}
EV	Qualcomm(R) Octa-core 1.5	2	Android 4.2.2	0,54	0,5	16,6
LAG	Intel(R) Dual-core 3.1	4	64-bit Win-7	0,36	0,38	11,5
ST/CS	Intel(R) Hexa-core 1.6	16	16 Win server 2012	0,3	0,31	8,6
AS/CA/RA	Intel(R) Hexa-core 1.6	16	16 Win server 2012	0,3	0,31	8,6

- Costs of the authentication phase and generation of keys

According to Table 5.8, the largest number of operations of the proposed protocol is concentrated on the entity of best computational properties, i.e., AS. Such a characteristic offers better performance and flexibility to the V2G network and avoids the overload of operations in elements of limited resources.

Table 5.8- Computational cost of the authentication phase

Protocol	Jie et. al[12]	Saxena et. al [13]	Proposed protocol
EV/PEV	$3nT_{mul} + nT_{pair} + nT_{exp}$	$nT_{mul} + nT_{pair} + 3nT_{exp}$	$4nT_{mul} + nT_{pair}$
ST/CS	$nT_{mul} + nT_{pair}$	--	--
LAG	$(n + 1)T_{mul} + nT_{pair} + nT_{exp}$	$(n + 1)T_{mul} + nT_{pair} + 5T_{exp}$	$(n + 5)T_{mul} + 1T_{pair}$
AS	--	--	$(2n + 15)T_{mul} + (n + 1)T_{pair}$
CA/RA	--	$(3n)T_{mul} + (3n)T_{exp}$	--

Figure 5.13 shows a comparison of the total computational cost of the authentication phase of the proposed protocol and the protocols of Jie et al. [12] and Saxena et al. [13]. Our protocol shows better computational performance than the protocol proposed by Jie et al. [12] when the number of EVs $n > 2$ and that of Saxena et al. [13] when $n > 6$.

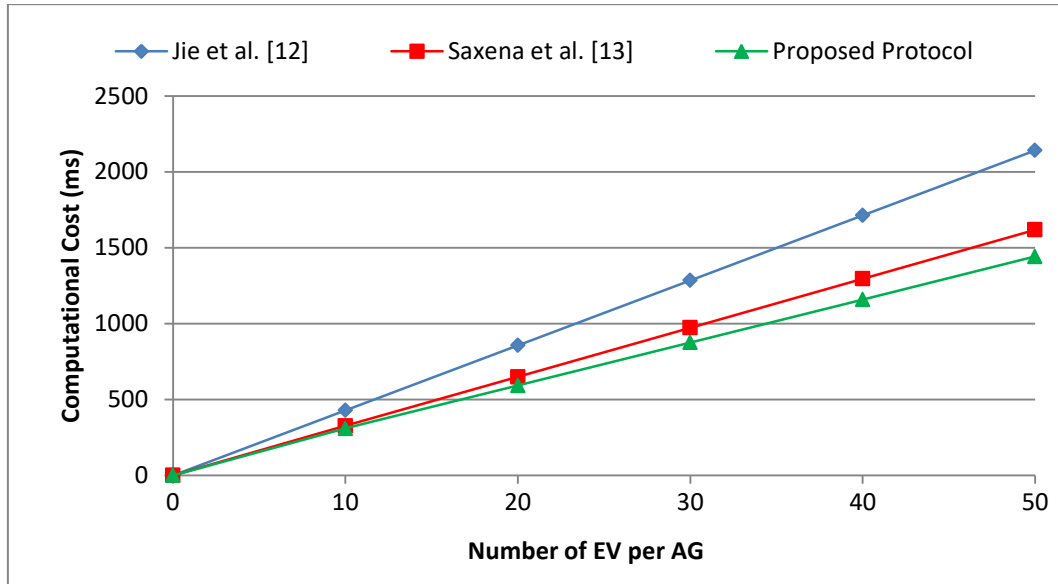
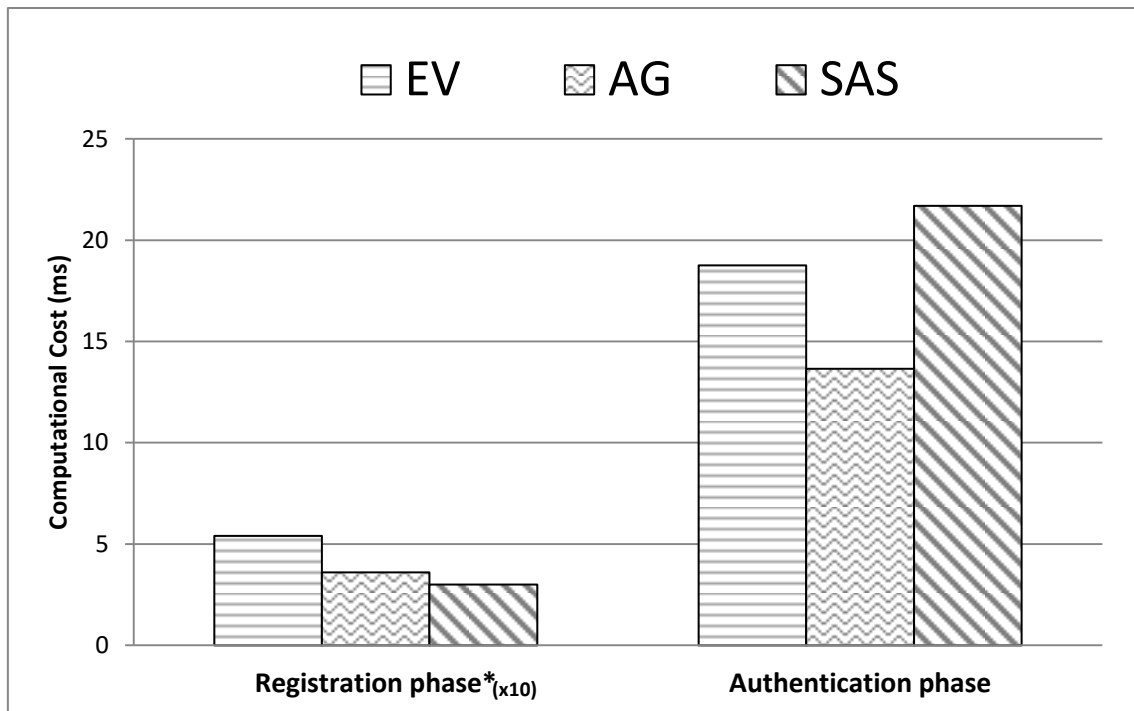


Figure 5.13- Comparison of computational costs among protocols

- Computational Cost per Entity of the Proposed Protocol

Figure 5.14 shows the comparison of the computational costs of the entities of the proposed protocol when an EV registers and authenticates in the V2G system. In the registration phase the EV, AG and SAS have the same number of operations to execute, but the computational cost of the EV is higher, since its processing power is lower than AG and SAS. SAS has a lower cost because its processing power is higher compared to AG.

In the authentication phase the computational cost raises considerably, due to the number of operations on each entity, as shown in Tables 7 and 8 for $n=1$. AG has the lowest computational cost, just for grouping the information of the EVs connected to it and sends that information to the SAS, so the number of operations that it executes are smaller in with the EVs and SAS. SAS concentrates several tasks involved in this phase, thus its computational cost is the largest.



* the original values were multiplied by 10 to better visualize the differences.

Figure 5.14- Computational Cost in Registration and Authentication phases, for entities of the proposed

c) Storage Cost

The next step was to compare the storage cost of the proposed protocol and the proposed ones by Jie et al. [12] and Saxena et al. [13]. In this comparison will be considered the parameters created in the authentication phase and that need to be stored to carry out the authentication process. Table 9 shows the comparison of storage costs in bits:

Table 5.9- Storage Cost of the Authentication Phase

Protocol	Jie et. al[12] (bit)	Saxena et. al [13] (bit)	Proposed protocol (bit)
EV/PEV	$896n$	$768n$	$640n$
ST/CS	$256n$	--	--
LAG	$394n + 640$	$640n + 128$	768
AS	--	--	$320n + 1088$
CA/RA	--	$256n$	--
Total	$1546n + 640$	$1664n + 128$	$960n + 1856$

In Table 10 and Figure 5.15 it can be seen that the storage cost of the proposed proposed is lower than the protocols of Jie et al. [12] and Saxena et al. [13] for $n \geq 3$. The best

performance in terms of storage is due to the cryptographic scheme, that involves the creation and storage of less data (bits) to carry out the authentication process.

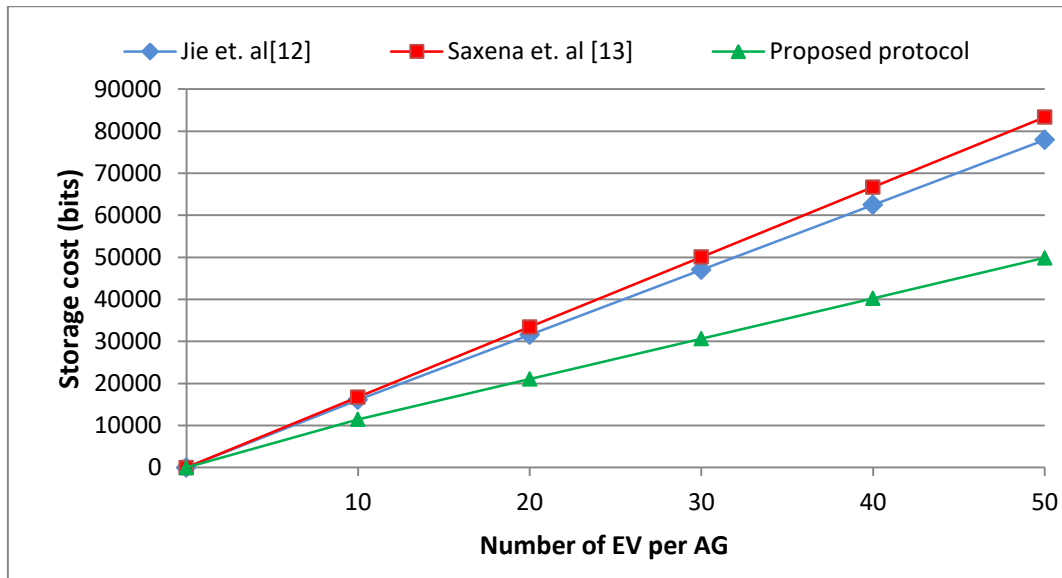


Figure 5.15- Storage Cost of the Protocols

5.7. Conclusions and Future Work

Due to the global need of reductions in air pollution, EVs have been a trend in research in many countries, as they can consume little or no petroleum, a scarce and non-renewable resource.

Part of the research related to EVs has been directed towards the creation of V2G networks for integrating EVs into SG networks. A fundamental part of the V2G network is the batteries of EVs, as they interact with an electricity network controlled by a bidirectional communication. Batteries can permit an EV to realize different functions within the V2G network, such as a provider, consumer or power storer.

Some security challenges in V2G communications involve preserving confidentiality and privacy of data, e.g. vehicle identity, user's identity, vehicle type, vehicle location, and other information to be protected. On the other hand, group-based organization of EVs [22] allows to improve energy distribution in SGs.

Part of the mentioned security challenges regards the authentication needs of EVs for their access to the V2G network. Some group-based authentication protocols have been proposed, however, their communication costs must be improved. Some of them also show computational overload in some elements of their infrastructure and a weak security analysis.

This chapter has introduced a new group authentication protocol for the V2G network based on ECDH and bilinear pairing. A brief description of some studies on security in V2G networks and solutions proposed for authentication in such networks are also provided.

In comparison with other proposals, our protocol shows better computational and communication costs and provides better results regarding security analysis. Moreover, it avoids centralization-related problems, due to a better distribution of the computational processing of operations in the devices and assures authentication of more entities.

We observe that the protocol proposed by Jie et al. [12] has a low number of messages exchanged among entities, but a high processing cost in devices of limited computational resources, as EVs and LAGs, due to the calculation of exponential functions. On the other hand, the use of asymmetrical encryption in the communication between EV and CA/RA decreases its efficiency.

The protocol proposed by Saxena et al. [13] has a high number of messages exchanged is also a high cost of processing concentrated in the LAG, due to the processes of verification and generation of keys that has to realize.

The AVISPA simulation tool formally proved the protocol is secure and guarantees successful authentication. It can meet the security and performance objectives and has proven a good choice in comparison to other authentication protocols for V2G networks.

Future work involves simulation of the protocol in a network simulator and its adaption for integration in the V2G network for the cloud. Another line of work involves authentication and authorization protocols for cyber physical systems (CPS) considering communication models such as the model presented in [23].

5.8.References

- [1] K. Shuaib, E. Barka, J. A. Abdella, F. Sallabi, M. Abdel-Hafez, Ala Al-Fuqaha, "Secure Plug-in Electric Vehicle (PEV) Charging in a Smart Grid Network", *Jurnal Energies*, v.10, 2017.
- [2] B. Vaidya, D. Makrakis, H. T. Mouftah, "Security Mechanism for Multi-domain Vehicle-to-Grid Infrastructure", *Conf. IEEE Global Telecommunication*, 2011.
- [3] A. Abdallah, X. Shen, "Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections", *IEEE Transactions on Vehicular Technology*, v. 66, No. 3, pp. 2615-2629, 2017.
- [4] H. Liu, H. Ning, Y. Zhang, Q. Xiong, L. T. Yang, "Role-Dependent Privacy Preservation for Secure V2G Networks in the Smart Grid", *IEEE Transactions on Information Forensics and Security*, v. 9, No. 2, pp. 208-220, 2014
- [5] N. Saxena, S. Grijalva, V. Chukwuka, A. V. Vasilakos "Network Security and Privacy challenges in Smart vehicle-to-grid" *IEEE Wireless Communications*, v.24, pp. 88-98, 2017.
- [6] H Wang, X Yu, H Song, Z Lu, J Lloret, F You, A Global Optimal Path Planning and Controller Design Algorithm for Intelligent Vehicles, *Mobile Networks and Applications*, 1-14. 2016
- [7] Keiko Karaishi, Masato Oguchi, Evaluation of Smart Grid Simulation System with Power Stabilization by EV, *Network Protocols and Algorithms*, Vol 5, No 1 (2013). Pp. 71-89
- [8] W. Han, Y. Xiao, "Privacy preservation for V2G networks in smart grid -A survey", *Computer Communications*, pp. 17-28, 2016.
- [9] W. Han, Y. Xiao, "IP2DM- integrated privacy-preserving data management architecture for smart grid V2G networks", *Wireless Communications And Mobile Computing*, v.16, pp. 2956-2974, 2016.
- [10] M. Tao; K. Ota; M. Dong, "Foud - Integrating Fog and Cloud for 5G-Enabled V2G Networks", *IEEE Network*, v. 31, pp. 8-13, 2017.
- [11] Shuaib, K.; Barka, E.; Abdella, J.A.; Sallabi, F.; Abdel-Hafez, M.; Al-Fuqaha, A. "Secure Plug-in Electric Vehicle (PEV) Charging in a Smart Grid Network" , *Secure Plug-in Electric Vehicle (PEV) Charging in a Smart Grid Network*", *Energies*, v.10, 2017.
- [12] C. Jie, Z. Yueyu1, S. Wencong, "An anonymous authentication scheme for plug-in electric vehicles joining to charging-discharging station in V2G networks" *China Communication*, v.12, pp. 9-19, 2015.
- [13] N. Saxena, B. J. Choi; S. Cho, "Lightweight Privacy-Preserving Authentication Scheme for V2G Networks in the Smart Grid" *IEEE Trustcom/BigDataSE/ISPA*, v.1, pp. 604-611, 2015.
- [14] Sania Yaqoob and Taeshik Shon, A Hybrid EV Authentication Approach in Smart Grid Based Distributed Network, *Ad Hoc and Sensor Wireless Networks*, Vol. 31, Number 1-4, Pp. 89-99, 2016.
- [15] J Lloret, P Lorenz, A Jamalipour, Communication protocols and algorithms for the smart grid, *IEEE Communications Magazine* 50 (5). 2012.

- [16] H. Liu; H. Ning, Y. Zhang, M. Guizani, “Battery Status-aware Authentication Scheme for V2G Networks in Smart Grid”, IEEE Transactions on Smart Grid, v.4, pp. 99-110, 2013.
- [17] Li, F., Xin, X. e Hu, Y. (2008) “Efficient Certificate – Based Singryption Scheme From Bilinear Pairings”, International Jurnal of Computers and Applications, v.30, No 2, 2008.
- [18] Menezes, Alfred. (2005) “An Introduction to Pairing-Based Cryptography”, Recent Trends in Cryptography, v. 477, p. 47-65.
- [19] M. Tao; K. Ota; M. Dong, Z. Qian, “AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks”, Journal of Parallel and Distributed Computing, 2017.
- [20] The AVISPA Project: European Union in the Future and Emerging Technologies (FET Open). Retrieved Nov 26, 2016, from <http://www.avispa-project.org>.
- [21] Z. A. Baig, A. R. Amoudi, (2013) “An Analysis of Smart Grid Attacks and Countermeasures”, Journal of Communications, v. 8, No. 8, 2013.
- [22] J Lloret, M Gilg, M Garcia, P Lorenz, A group-based protocol for improving energy distribution in smart grids, Communications (ICC), 2011 IEEE International Conference on, 1-6. 2011.
- [23] Jafar Rasouli, Seyed Ahmad Motamedi, Mohamad Baseri and Mahshad Parsa, A Reliable Communication Model based on IEEE802.15.4 for WSNs in Smart Grids, Ad Hoc and Sensor Wireless Networks, Vol. 39, Number 1-4 (2017). Pp. 313-343.

Chapter 6

Conclusion

The "Smart Grid" (SG), or smart electrical network, refers to the application of technologies that enable the real-time monitoring of the equipment and processes of generation, transmission and distribution of electric energy in an integrated way. SG's represent a significant change in paradigm for the electric energy sector, and are expected to optimize the production and distribution of electric energy based on better management and automation processes by the extensive utilization of information and communication technologies.

The development of a secure smart grid imposes new communication requirements to the power delivery system, regarding protocols, delays, bandwidth and costs. Thus, since the adequate exchange of messages and storing of data impact the control and management of the network, both security and reliability of the data must be always assured by the infrastructure of the smart electric network.

Several security problems can occur in such a relatively new environment. For example, a denial of service attack can severely harm critical infrastructures of electricity of a city or a country. Some people's habits, including presence or absence of residents and number of residents in a house can be determined by an intruder who accesses data related to the consumption of electrical energy. Moreover, financial losses can occur as a consequence of alterations in smart meter data. Last but not least, power grids are a major resource to the national defense.

This dissertation has focused, initially, on some basic and advanced concepts regarding new techniques of protection, mainly related to confidentiality, privacy and integrity. A main objective and some secondary objectives were established.

We consider that the main objective was reached, by the proposal of authentication and authorization protocols in different scenarios of the SG networks, with characteristics of preserving information security and performing well in comparison to other protocols already published. Three protocols were proposed, and each protocol was compared with at least two other proposals recently published, aiming to meet previously established secondary objectives.

For each protocol, a different scenario was considered, having in common the same architecture of SG networks, but encompassing specific needs, according to the specific scenario, respective entities and possible threats and vulnerabilities. Thus, the protection against possible attacks was designed, using resources such as bilinear pairing, ECDH, hash functions and temporary identities, among others.

In the first scenario, the need for secure control and management of the electricity network equipment by the employees of the energy supply company was considered; a protocol was designed, considering roles and attributes of the mentioned people, leading to protection of the devices that are part of the management system and confidential data (system configuration, user data, among others) of the Smart grid. The protocol was based on cryptographic techniques such as bilinear pairing and Certificate-Based Signcryption (CBS) and the RABAC access control model. An interesting feature of this protocol is the use of a second OTP authentication factor for user authentication, in addition to using bilinear pairing for identity verification.

In the second scenario, the need for secure acquisition of measurement data in the Advanced Metering Infrastructure was considered, with a computational cloud used to provide better processing capability, and better storing resources for data related to consumption and other data needed for control and management tasks. A second protocol was then designed considering the large number of Smart Meters that have to connect to the Smart grid, leading to the protection of confidentiality and privacy of users' consumption data. Some interesting characteristics of this protocol are the use of aggregators to reduce the load in the communications of the SG system and the integration of the cloud in the architecture to support the growth of the computational requirements due to the exponential growth of the demand.

In the third scenario, the need for secure charging/discharging plug-in electrical vehicles was considered, for the sake of the optimization of both supply and demand of energy in the SG network. A third protocol was designed, with characteristics to protect the privacy and confidentiality of the data of the users of electric vehicles, emphasizing the great amount of electric vehicles that will need to charge or charge the energy of their batteries. Some interesting features of this protocol are the creation of a session key from a bilinear pairing operation, the use of a broadcast message to send authentication data and data for session key generation, use of double authentication factor to generate the session key, and propose a decentralized authentication server scheme.

The three proposed protocols were evaluated and compared with other proposals in two dimensions:

- a) Security properties;
- b) Computational and communication costs.

For the first dimension, the protection against a set of possible attacks was considered, aiming to reach security properties and improve characteristics of other proposals, under specific assumptions related to security or insecurity of communication channels and other resources. Then, security properties related to the resistance against some attacks and other more general properties such as integrity and privacy were investigated; the set of attacks included the most common attacks, such as redirecting, Man-in-the-Middle and repetition, among others.

For the second dimension, two types of costs were considered:

- Computational costs, involving the utilization of processing resources at the entities, such as smart meters, IED's, authentication servers and electric vehicles; these costs were evaluated considering computational time for the operations necessary for implementation and use of the protocol; some testbeds recently published in the literature were considered.
- Communication costs, involving the set of messages necessary for each protocol and respective number of bits, that would represent the bandwidth necessary to the implementation of the protocol.

Complementing the first dimension of evaluation, a relevant task was accomplished: the formal validation of the proposed protocols. For this, a tool named AVISPA, a high-level language (HLPSL), a graphical animator (SPAN) and some back-ends were used. For some possible attacks and properties, the protection provided by the proposed protocols was formally assured.

APPENDIX I - Letter of Acceptance of article at the XXXV SBRC 2017. O Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2017)

De: SBRC 2017 - CoUrb <courb.sbrc@gmail.com>
Data: 24 de abril de 2017 21:39
Assunto: Your SBRC 2017 - CoUrb paper 168432
Para: lfroman@aluno.unb.br
Cc: Paulo Gondim <prgond@gmail.com>, Ana Paula Golembiouski Lopes <anagolembiouski@aluno.unb.br>

Prezado(a) Luis Fernando Arias Roman:

Parabéns! Temos a satisfação de informar que o seu artigo 168432, "Protocolo de Autenticação e Autorização em ?Smart Grids? para Cidades Inteligentes" foi aceito para apresentação em forma de pôster e publicação no SBRC 2017 - CoUrb.

Recebemos um número relativamente alto de submissões para a primeira edição do Workshop, o que inevitavelmente tornou o processo de revisão bastante competitivo. Dos 54 artigos submetidos, 22 foram recomendados para aceitação, correspondendo a uma taxa de aceitação aproximada de 40%. Dos 22 artigos recomendados, 14 artigos foram aceitos para apresentação oral e 8 artigos para apresentação em forma de pôster.

As revisões relativas ao seu artigo estão no final desta mensagem e também podem ser acessadas em <https://jems.sbc.org.br/PaperShow.cgi?m=168432>. Ao preparar a versão final do seu artigo, observe as sugestões apresentadas pelos revisores.

O artigo final deve ter no máximo 14 páginas, em formato PDF, e estar PLENAMENTE de acordo com o formato da SBC, disponível em <http://www.sbc.org.br/documentos-da-sbc/summary/169-templates-para-artigos-e-capitulos-de-livros/878-modelosparapublicaodeartigos> (Templates para Artigos e Capítulos de Livros).

Para completar o processo você deve fazer o "upload" dos seguintes arquivos via sistema JEMS, IMPRETERIVELMENTE até o dia 29/04/2017:

- 1) Versão final do artigo
- 2) Formulário de direitos autorais assinado disponível em [http://www.sbc.org.br/documentos-da-sbc/summary/164-publicacoes/1020-contrato-de-cessao-de-direitos-autorais\(Contrato de cessão de direitos autorais\)](http://www.sbc.org.br/documentos-da-sbc/summary/164-publicacoes/1020-contrato-de-cessao-de-direitos-autorais(Contrato%20de%20cess%C3%A3o%20de%20direitos%20autorais)).

A publicação do artigo nos Anais está condicionada à INSCRIÇÃO de pelo menos um dos autores do artigo no CoUrb 2017 (e por consequência, no SBRC 2017) e ao comprometimento dos mesmos com a APRESENTAÇÃO em forma de pôster no dia do Evento. Caso isso não seja possível, manifeste-se por e-mail ao coordenador o quanto antes.

Atenciosamente,
Leandro Villas (UNICAMP)
Thiago Henrique Silva (UTFPR)
Daniel Ludovico Guidoni (UFSJ)
Bruno Yuji Lino Kimura (UNIFESP)
Roberto Sadao Yokoyama (UTFPR)

APPENDIX II – Paper “Protocolo de Autenticação e Autorização em “Smart Grids” para Cidades Inteligentes”. Submitted at the Event (SBRC 2017)

Protocolo de Autenticação e Autorização em “Smart Grids” para Cidades Inteligentes

Luis Fernando Arias Roman¹, Paulo Roberto de Lira Gondim², Ana Paula Golembiowski Lopes³

Departamento de Engenharia Elétrica – Universidade de Brasília (UnB)
Campus Universitário Darcy Ribeiro – 70910-900 – Brasília – Brasil

{lfroman, anagolembiowski}@aluno.unb.br, pgondim@unb.br

***Abstract.** One of the services that has been considered for the implementation of smart cities is Smart Grid, where is essential to guarantee the integrity, accessibility and confidentiality of the data. In this work, a protocol of authentication and authorization of users is proposed to mitigate the internal and external threats. Security and performance analyzes show that the proposed protocol is more efficient compared to existing systems, considering security properties and computational and communication costs.*

***Resumo.** Um dos serviços que tem sido considerado para a implementação de cidades inteligentes é Smart Grid, onde é essencial garantir a integridade, acessibilidade e confidencialidade dos dados. Neste trabalho, propõe-se um protocolo de autenticação e autorização de usuários para mitigar as ameaças internas e externas. Análises de segurança e desempenho mostram que o protocolo proposto é mais eficiente em comparação com os sistemas existentes, considerando propriedades de segurança e custos computacionais e de comunicação.*

1. Introdução

De modo geral se pode descrever uma "cidade inteligente" como uma área urbana que, com ajuda da tecnologia, serve de suporte ao atendimento a necessidades de empresas, instituições e, especialmente, os cidadãos. O rótulo citado pressupõe a obtenção de uma melhor eficiência para o planejamento urbano através de uma variedade de tecnologias [Kamienski 2016], dentre as quais as Tecnologias da Informação e Comunicação (TIC) desempenham um papel fundamental para o seu desenvolvimento. As TIC's podem ser utilizadas de forma a possibilitar o atendimento a necessidades de escalabilidade, do meio ambiente e de segurança, favorecendo a construção de soluções inovadoras.

Cidades inteligentes dependem, dentre outros fatores, da utilização de sistemas capazes de tratar adequadamente a demanda, a geração e a distribuição de energia elétrica, de forma integrada com outros sistemas e redes. Smart Grid (SG) constitui um agregado

de tecnologias e subsistemas, que pode ser utilizado visando a implementação de cidades inteligentes, pois integra sistemas avançados de energia, redes e tecnologias de comunicação.

O emprego de soluções baseadas em SG permite que redes elétricas funcionem de forma mais eficiente, produtiva, sustentável e transparente. Todavia, dentre os diversos problemas possíveis, inclui-se o de segurança da informação, em decorrência de ameaças e ataques que afetam a confidencialidade, a integridade, a acessibilidade, a proteção e a privacidade dos dados.

Como possíveis resultados de ataques à segurança de SG, a integridade, a disponibilidade e a confidencialidade das informações armazenadas ou em trânsito podem ser comprometidas, levando por exemplo à modificação de dados sem autorização, gerando latência na rede e possivelmente expondo informação dos clientes.

Em uma visão ampla das necessidades de autenticação e autorização em SG, é necessário considerar os vários tipos de usuários, tais como empregados (EMP), engenheiros fornecedores (*vendors engineers* ou VE), pessoal de manutenção (MP) e funcionários de segurança (*security office* ou SO). Assim, cada um desses usuários pode dispor de acesso a algumas possibilidades de uso do sistema, tais como leitura, leitura-escrita, e adição-modificação-apagamento).

Nesse contexto a autenticação e autorização de usuários em SG é um desafio, devido ao fato de que os dispositivos e demais recursos podem ser acessados tanto localmente quanto remotamente via Internet, sendo também necessário tratar o acesso aos recursos de forma específica para as necessidades de natureza funcional de cada usuário. Dessa forma, somente usuários autenticados devem poder executar as ações devidamente autorizadas para os dispositivos (atribuídos com base nas funções de cada usuário) e demais recursos, e de uma forma controlada e escalável.

No presente documento se propõe um protocolo que realiza autenticação mútua e autorização entre o usuário e um servidor de autenticação de SG. O protocolo é parcialmente baseado em [Vaidya 2013] e [Saxena 2016], e realiza autorização dinâmica para cada papel de usuário, usando emparelhamento bilinear e alguns conceitos e técnicas presentes no sistema criptográfico *Certificate-Based Signcryption (CBS)* [Li 2008].

Após a autenticação, uma autorização pode ser provida, sendo mantida por tempo limitado para que cada usuário possa executar apenas as ações que são permitidas, considerando as permissões de acesso e a respectiva validade. O protocolo proposto se baseia em autenticação de dois fatores: o primeiro consiste na verificação de identidade, enquanto o segundo é uma *One-Time Password* (OTP), enviada via terminal celular ao usuário que está acessando o dispositivo. Com o OTP o usuário também pode realizar a verificação de validade do remetente. Além disso, no protocolo é compartilhada uma chave de sessão entre o dispositivo e o usuário mediante o uso de ciframento baseado em certificado.

O manuscrito está organizado da seguinte forma: na seção 2 são expostos conceitos básicos; na seção 3 são descritos alguns trabalhos relacionados com a autenticação e autorização do usuário em SG. Na seção 4 é descrito o protocolo proposto. Na seção 5 é feita a análise de desempenho do protocolo proposto, bem como é caracterizado o

atendimento a propriedades de segurança. Por fim, na seção 6 são apresentadas as conclusões, bem como são indicados trabalhos futuros.

2. Conceitos Básicos

2.1. Arquitetura de um SG

A seguir se descrevem terminologias da rede SG em geral, que permitam tratar as arquiteturas que serão usadas como base, bem como favorecer o entendimento da proposta de protocolo.

- **SCADA** (*Supervisory Control And Data Acquisition*):
É um sistema que capta a informação de diversas fontes de produção e consumo de energia, para gerar indicadores que permitam tomar decisões automatizadas e controladas no sistema elétrico.
- **IED** (*Intelligent Electronic Device*)
Um IED é qualquer equipamento controlado por microprocessador conectado para interagir com um sistema de energia, por exemplo, equipamentos para monitoramento, equipamentos para controle ou proteção de circuitos, equipamentos distribuição ou disseminação de energia elétrica, etc.
- **SM** (*Smart Meter*)
São equipamentos que tem sensores para medir e enviar informação da eletricidade consumida para a companhia de energia. Também tem a capacidade de receber informação com instruções.
- **OFEs** (*Outdoor Field Equipment*)
São equipamentos da rede SG alocados na rua, como por exemplo: transformadores, agregadores (gateways), etc.
- **AS** (*Authentication Server*)
São servidores que validam as credenciais e identidade dos usuários, e também armazena os atributos e papéis que correspondem a cada um de eles. Para um sistema de grande tamanho como SG se pode ter uma arquitetura distribuída com um AS Central (ASc) que pode estar localizado em uma central de operações, e conectados a ele vários AS que podem estar na subestação (ASs).

Uma possível arquitetura de SG é a apresentada na Figura 1. Esta arquitetura esta composta de SMs instalados nas casas dos usuários, OFEs distribuídos em diferentes lugares de uma cidade, IEDs localizados nas subestações. Estes dispositivos podem ser acessados por diferentes usuários (MP, VE, SO) de forma presencial ou remota. Assume-se que se um usuário tem acesso ao dispositivo de forma física ou sem fio, o dispositivo tem mecanismos que garantem a integridade da informação.

Por outro lado se tem um Centro de Controle (CC), onde esta instalado o ASc encarregado de concentra toda a informação enviada de forma segura pelos ASs. por meio de uma chave pre-compartilhada e diferente para cada enlace. A comunicação no sistema SG esta suportada por DNP3 or IEC 61850 representadas por linhas laranja. Além disso, as comunicações também são sustentadas por tecnologias WAN / Celular para suportar a rede sem fio.

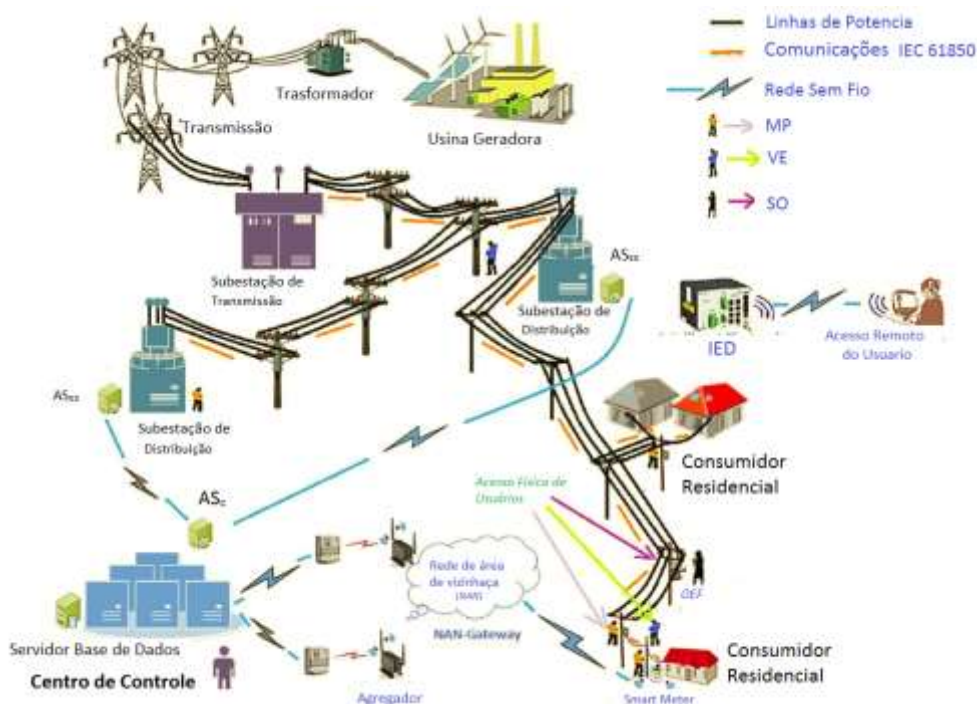


Figura 1. Arquitetura Sistema *Smart Grid* (adaptada de [Saxena 2016])

2.2 Controle de Acesso

O Controle de acesso a sistemas é fundamental para garantir a confiabilidade, integridade e disponibilidade destes. Os controles podem ser administrativos (políticas empresariais), lógicos (protocolos de autenticação e autorização) ou físicos (restrição de ingresso a zonas críticas mediante portas). O controle de acesso tem vários modelos como por exemplo o *Role-Based Access Control* (RBAC) em que uma autoridade central determina/gerencia quais usuários podem ter acesso aos objetos controlados. A autorização é dada baseando-se no papel (*role*) que o usuário desempenha na organização (*role-based*) ou responsabilidades deste usuário na organização (*task-based*). Outro dos modelos é o *Attribute-based Access Control* (ABAC) onde define-se permissões se baseando em características relevantes de segurança, conhecidas como atributos. No entanto, um número potencialmente grande de atributos deve ser entendido e gerenciado, além disso, os atributos só têm significado até que tenham uma associação com um usuário, objeto ou ambiente [Coyne 2013].

2.3 Descrição de Ataques

Todo SG é vulnerável a ataques sobre seus diferentes componentes, desde os SM até o SCADA, portanto as medidas de proteção devem abordar toda a infraestrutura da SG. Por exemplo, um atacante interno pode ingressar a um SM e modificar as leituras ou obter informação privada do usuário dono da SM. Da mesma forma pode obter informação de preços da energia, informação da infraestrutura de rede e outras informações comunicadas por protocolos usados por SG como DNP3 (*Distributed Network Protocol*), EMS (*Energy Management System*), ICCP (*Intercontrol Center*

Communication Protocol) e OSGP (*Open Smart Grid Protocol*) [Lopes 2016].

Dispositivos como SM, IED e OFE da SG utilizam várias senhas locais com diferentes privilégios dependendo dos papéis do usuário, para permitir a autenticação e autorização de acesso dos trabalhadores que usam estes dispositivos. Devido ao grande número de dispositivos, as senhas geralmente são compartilhadas entre vários usuários, gerando muitos problemas de segurança no sistema.

Como possíveis exemplos de ataques a um SG, um intruso pode executar um ataque *Man-in-the-Middle* criando uma conexão ativa entre o usuário e um servidor, fazendo-os acreditar que estão se comunicando diretamente entre si de forma segura. Outro ataque que um intruso pode executar é um ataque de repetição que ocorre quando um intruso espia o canal de comunicação para obter parâmetros importantes e usá-los para representar uma das entidades envolvidas nas execuções de processo subsequentes. Um invasor também pode executar um ataque de representação que ocorrem quando um dispositivo falso consegue fingir que é genuíno e recebe as mensagens destinadas a este dispositivo genuíno. A mudança de parâmetros de segurança pode ser feita por atacantes internos ou externos, portanto um usuário autorizado pode alterar os parâmetros de segurança do sistema SG ou o dispositivo a fim de obter acesso ou mais privilégios sobre ele. Também, o usuário pode adulterar o SM para reduzir o custo do uso da energia elétrica. Um dos mais importantes requerimentos de segurança é a prevenção contra um ataque de repúdio onde um atacante pode alterar os dados e, em seguida, negá-lo. Este ataque pode ser intencionalmente realizado por um atacante interno ou externo [Stallings 2014].

3. Trabalhos Relacionados

Foram considerados trabalhos de pesquisa propondo soluções de segurança contra ataques que podem ser provocados por operadores, pessoal de manutenção e intrusos, dentre outros. Assim, nosso foco envolve trabalhos relativos a protocolos que permitam controlar o acesso a recursos e dispositivos, bem como autorizar as atividades de cada usuário.

[Vaidya 2013] apresenta proposta que considera um servidor centralizado chamado SSC (*Substation Controller*) que tem as funções de autenticação de usuários, atribuir certificados de atributo aos usuários e manter registros de acesso. O autor considera alguns desafios importantes das redes SCADA, como as restrições que incluem recursos computacionais e de armazenamento limitados de dispositivos de campo, transmissão de dados de baixa taxa e a necessidade de respostas com baixa latência de dispositivos em toda a rede.

O protocolo proposto pelo autor tem as seguintes características: usa o sistema criptográfico de chave pública (*PKC*) baseado em curva elíptica ou ECC (*Elliptic curve Cryptography*), que executa um Protocolo de prova de zero-conhecimento com verificação assistida por servidor ou SAV (*Server Aided Verification*), e tem um Certificado de Atributos ou AC (*Attribute Certificate*) [Brown 2009] para a autorização de serviços.

No trabalho de [Saxena 2016] é desenvolvido um protocolo de autenticação mútua entre o usuário e o servidor, e uma autorização dinâmica para cada papel do usuário calculando um valor *hash* com base em seus atributos. O autor considerou uma arquitetura de SG constituído por IED, SMs, OFEs, e um Servidor de Autenticação

Central ou ASc que interconecta os servidores de autenticação das subestações ou ASs. Neste protocolo é estabelecida a autenticação de dois fatores. Primeiro, a autenticação é realizada através da verificação da identidade de cada usuário no servidor da subestação. Em seguida uma senha OTP é enviada ao telefone celular do usuário a fim de verificar a identidade do usuário que esta acessando ao dispositivo. Finalmente uma chave secreta é compartilhada entre o usuário e o dispositivo para uma comunicação segura usando a técnica de emparelhamento bilinear.

Outros trabalhos como [Cheung 2015], propõe um esquema de controle de acesso para redes SG chamado *Smart-Grid Operation-based Access Control* (SOAC) e [Lee 2015] que propõe a implementação de *Role-Based Access Control* (RBAC) baseado na norma da *International Electrotechnical Commission* (IEC) 62351, utilizando *Extensible Access Control Markup Language* (XACML).

Neste trabalho considera-se o emprego de RBAC para controle de acesso aos componentes e recursos do sistema de SG e o ABAC para validação da identidade do usuário.

4. Protocolo Proposto.

Esta seção apresenta o protocolo proposto, visando prover autenticação e um papel dinâmico para o controle de acesso baseado em atributos, para atingir as propriedades de segurança de maneira mais eficiente em termos de custos computacionais e comunicação, comparado com outros protocolos propostos que tratam problemas similares. O protocolo é parcialmente baseado em [Vaidya 2013] e [Saxena 2016], como também de alguns conceitos e técnicas presentes nos sistemas criptográficos *Certificate-Based Signcryption* (CBS) [Li 2008]. e *Pairing-based cryptography* (PBC) [Menezes 2005].

Cada usuário tem um papel (dependendo de suas funções) que é atribuído por um AS (Authentication Server). Todo o sistema de autenticação e autorização está baseado no *Certificate-Based Signcryption* (CBS) com emparelhamento bilinear [Li 2008]. Em seguida se descrevem as premissas da proposta, com base na arquitetura indicada na figura 1.

- Em caso de acesso físico dos dispositivos, uma interface de usuário fornece entrada/saída de dados para cada dispositivo e tem a capacidade de fazer cálculos computacionais.
- O cenário apresentado é semelhante para IEDs, SMs, e OFEs. Neste artigo se representara o protocolo com os IEDs, mas pode ser facilmente estendido para os outros tipos de dispositivos.
- Cada usuário faz o registro de seus dados (chave publica, identidade, papel, telefone, Etc.) presencialmente na correspondente subestação.
- O canal de comunicação entre um dispositivo e um servidor de autenticação (ASs) é segura.
- Assume-se que o relógio dos dispositivos é mantido sincronizado com o relógio do sistema.

A proposta tem quatro fases: 1a) inicialização do sistema; 2a) registro dos usuários e

das subestações; 3a) controle de acesso a dispositivos; 4a) verificação da identidade das entidades. Adicionalmente na tabela 1 são descritos os símbolos e seu comprimento em bits, usados neste trabalho.

Tabela 1. Símbolos e Custo em bits [Saxena 2016].

Símbolo	Descrição	Comprimento (bits)
Nome	Nome de usuario	128
ID	Identificação do usuario	128
$H()$	Função hash	64
x	Chave privada	128
y	Chave publica	128
k	Chave de sessão	128
Papei	Papel de usuario	64
L	Localização do usuário	32
Departamento	Departamento do usuario	16
T	<i>Token</i>	3
t	<i>Timestamp</i>	64
*	<i>Operador Multiplicação</i>	-
\hat{e}	<i>Emparelhamento Bilinear</i>	-
ASss	<i>Servidor de Autenticação da Subestação</i>	-
Cert	<i>Certificado Digital</i>	128
P	<i>Ponto da Curva Eliptia</i>	128
\oplus	<i>Operador XOR</i>	-

1ª. Fase: Inicialização do sistema [Menezes 2005]:

Escolhem-se G , G_T dois grupos cíclicos de ordem q , e P um elemento gerador do grupo G . se supõe que G e G_T estão relacionados com um emparelhamento, não-degenerativo e com um mapa bilinear que pode-se computar eficientemente $e : G \times G \rightarrow G_T$ tal que $\hat{e}(P, P) \neq 1_{G_T}$ e $\hat{e}(aP_1, bQ_1) = \hat{e}(bP_1, aQ_1) = \hat{e}(P_1, Q_1)^{ab} \in G_T$ para todo $a, b \in \mathbb{Z}_q^*$ e todo $P_1, Q_1 \in G$. Além disso se definem as funções hash do sistema: $H_1: \{0,1\}^* \rightarrow G$, $H_2: \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ e $H_3: G_1 \rightarrow \mathbb{Z}_q^*$.

Por fim o servidor de autenticação central (ASc) e todos os servidores das subestações (ASss) acordam uma curva elíptica sobre um campo finitos $E(F_q)$ e se publicam os parâmetros $\{ G, G_T, \hat{e}, P, H_1, H_2, H_3 \}$.

Com os parâmetros públicos os ASss das subestações escolhem uma chave privada $x_{ss} \in \mathbb{Z}_q^*$, e calcula sua chave publica $y_{ss} = x_{ss} * P$, a fim de publicar esta chave junto à identidade da subestação (IDss).

2ª. Fase: Registro de Usuários e Sub-estações

Todos os usuários e dispositivos tem que fazer um cadastro presencial na subestação atribuída. O cadastro de um usuário inicia quando ele escolhe uma identidade ID_u e uma chave privada $x_u \in \mathbb{Z}_q^*$, em seguida calcula uma chave publica $y_u = x_u * P$. O usuário envia mensagem que contem a chave publica e a identidade do usuário $\{ y_u, ID_u \}$ ao ASss. O ASss guarda os dados recebidos y_u e ID_u , e calcula $h_u = H_1(ID_u)$, para verificações posteriores. Além disso, o ASss associa os atributos do

usuário como nome, numero de telefone, dependência, papel. Seguidamente o ASss envia uma mensagem que contem a confirmação do papel assignado e o valor *hash* de sua identidade {papel, h_u }.

Para o cadastro para um dispositivo que faz parte da subestação, o primeiro que ele faz é escolher uma identidade (ID_{IED}), depois escolhe um numero aleatório $x_{IED} \in Z_q^*$ que será sua chave privada e com ela calcula uma chave publica $y_{IED} = x_{IED} * P$, O IED envia mensagem que contem a chave publica e a identidade do dispositivo $\{y_{IED}, ID_{IED}\}$ ao ASss. O ASss guarda os dados recebidos y_{IED} e ID_{IED} , e calcula $P_{IED} = H_1(y_{ss}, y_{IED})$, e $Cert_{IED} = x_{ss} * P_{IED}$. Por fim o ASss envia uma mensagem $\{Cert_{IED}, P_{IED}\}$ ao IED que certamente que tem que ser guardado no dispositivo, além disso, o certificado $Cert_{IED}$ é publicado na rede.

3ª. Fase: Controle de Acesso a Dispositivos

Esta fase inicia quando o usuário calcula um desafio $S_u = x_u * y_{ss}$, e enviando um mensagem $\{S_u, y_u, L, ID_{IED}, t_1, H_{m1}\}$ ao IED_i onde L é a localização do usuario, ID_{IED} é a identidade do dispositivo a ingressar, um t_1 é um *Timestamp* da criação da mensagem e H_{m1} um *hash* da mensagem para garantir a integridade.

Quando o IED_i recebe o mensagem, calcula com os valores recebidos um *hash* $H'_{m1} = H_1(S'_u, y'_u, L', ID'_{IED}, t'_1)$, e compara $H_{m1} =? H'_{m1}$, se os valores são diferentes o IED_i termina a conexão, pelo contrario, encaminha o mensagem $\{S_u, y_u, L, IED_i, t_2\}$ ao ASss, onde t_2 é um novo valor de *timestamp*.

O ASss procura a identidade do usuário ID_u comparando a chave publica recebida y_u com a chaves públicas alanceadas na fase de registro, se não encontra uma chave publica igual à recebida o ASss encaminha o mensagem $\{y_u, IED_i\}$ ao ASsc para procurar a identidade e permissões do usuário no registro de todo o sistema, se o ASsc não acha a identidade do usuário ou o não tem permissões sobre o dispositivo, envia uma mensagem ao ASss para fechar a conexão, pelo contrario, envia uma mensagem ao ASss que contem a identidade do usuário e o papel que tem atribuído $\{ID_{IED}, Role\}$. ASss verifica se o usuário tem uma sessão ativa no sistema, em caso de ter alguma, o ASss compara os dados da localização do mensagem recebido com a localização da sessão ativa $L =? L'$, se são diferentes a conexão é fechada, de outro modo calcula o desafio $S'_u = x_{ss} * y'_u$, e compara $S'_u =? S_u$, se da certo, escolhe um *token* T e calcula $P_A = H_1(T || Y_{ss} || ID_u || Role || L)$, e um certificado do usuario $Cert_u = x_{ss} * P_A$, e envia o mensagem $\{Cert_u, P_A, Role, T, t_3\}$ ao IED_i , onde t_3 e o novo *timestamp* do mensagem. Simultaneamente envia o *token* T ao usuário mediante uma mensagem de texto (*SMS*) ao telefone registrado.

O IED_i recebe o mensagem e escolhe $r \in Z_q^*$ e calcula: $X_1 = r * P_A$; $X_2 = r * y_{IED}$; $w_1 = r * x_{IED} * y_u$, escolhe aleatoriamente uma chave de sessão suficiente mente grande $K_s \in Z_q^*$, e calcula $h = H_1(X_1 || X_2 || K_s)$, $z = (r + h) * Cert_u + w_1$, $w_2 = r * Cert_u * P_{IED}$, e $\varphi = H_2(w_1 || w_2 || T) \oplus (z || ID_{IED} || K_s)$, IED_i envia o mensagem $\{\varphi, X_1, X_2, t_4\}$ ao usuário, onde t_4 e um novo *timestamp* do mensagem.

Para recuperar a chave de sessão que esta na mensagem, o usuário tem que calcular os seguintes valores: $W_1 = x_u * X_2$; $W_2 = X_1 * Cert_{IED}$, e faz uma operação *xor* da seguinte forma $\varphi \oplus H_2(W_1 || W_2 || T) = (z || ID_{IED} || K_s)$, onde T é o *token* enviado ao usuário mediante uma mensagem de texto (*SMS*) ao telefone registrado e K_s é a uma chave simétrica para a comunicação entre o usuário e dispositivo. Na Figura 2 se

amostra graficamente as mensagens trocadas, variáveis calculadas e verificações feitas na fase 2.

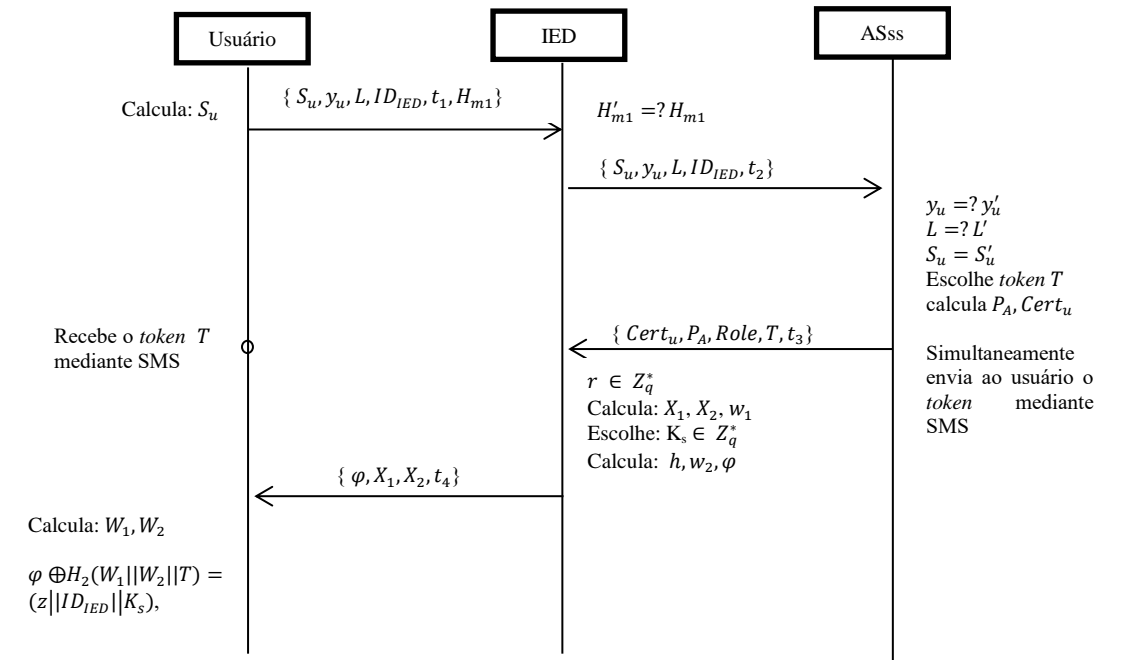


Figura 2. Fase de acesso protocolo proposto

4ª Fase: Verificação

Para verificar a mensagem recebida pelo usuário, ele tem que fazer os seguintes cálculos: $P'_A = H_1(T || Y_{SS} || ID_u || Role || L)$; $h = H_1(X_1 || X_2 || K_s)$, onde X_1 e X_2 são os valores recebidos no mensagem e K_s e a chave de sessão achada no mensagem. Depois de calcular os valores o usuário tem que fazer a seguinte verificação: $\hat{e}(z, P) = \hat{e}(X_1 + h * P_A, y_{SS}) \hat{e}(X_2, y_u)$. Esta comparação é baseada no encadeamento a seguir:

$$\begin{aligned}
 \hat{e}(z, P) &= \hat{e}((r + h) * Cert_u + w_1, P) \\
 &= \hat{e}((r + h) * Cert_u, P) \hat{e}(w_1, P) \\
 &= \hat{e}((r + h) * x_{SS} * P_A, P) \hat{e}(r * x_{IED} * y_u, P) \\
 &= \hat{e}(r * P_A + h * P_A, y_{SS}) \hat{e}(r * x_{IED} * y_u, P) \\
 &= \hat{e}(X_1 + h * P_A, y_{SS}) \hat{e}(r * x_{IED} * y_u) \\
 &= \hat{e}(X_1 + h * P_A, y_{SS}) \hat{e}(r * y_{IED}, y_u) \\
 &= \hat{e}(X_1 + h * P_A, y_{SS}) \hat{e}(X_2, y_u)
 \end{aligned}$$

5. Análises de Segurança e de Desempenho.

Apresentam-se aqui as análises de segurança e de desempenho do protocolo proposto, como também uma comparação de este com os protocolos apresentados em [Vaidya 2013] e [Saxena 2016], já que, consideram a autenticação entre usuário e servidor ao intentar acessar um dispositivo da rede SG.

5.1. Análise de Segurança

Nesta subseção será analisadas a autenticação, o estabelecimento de chave de seção a preservação da privacidade e a resistência de diferentes ataques do protocolo proposto.

- 5) Autenticação Mútua: a autenticação mútua é estabelecida entre o usuário (MP, EV, etc.) e o ASs, autentica ao usuário verificando o $S_u = x_{ss} * y'_u$, e o cada usuário autentica ao ASs mediante o uso do *token T* na fase de cálculo da chave de sessão (onde também podem verificar a identidade da subestação) e na fase de verificação usando a chave pública y_{ss} .
- 6) Estabelecimento de chave de sessão: cada chave de sessão K_s é gerada aleatoriamente e compartilhada durante a autenticação, portanto é válida só durante a sessão.
- 7) Preservação da privacidade: a identidade do usuário não é trocada nos mensagens e é preservada de maneira segura nas bases de dados dos servidores de autenticação.
- 8) Proteção da integridade: No protocolo proposto se fornece proteção de integridade usando funções *hash* em cada mensagem transmitido pela rede. Se um adversário intercepta a mensagem e intencionalmente faz mudanças a qualquer parâmetro transmitido o valor de *hash* da mensagem não irá coincidir no receptor e a ligação será terminada.
- 9) Prevenção contra ataques

O protocolo proposto resiste aos seguintes ataques:

- Ataque de Personificação: um atacante precisa conhecer a identidade e a chave secreta do usuário vítima. No entanto, não pode obter o parâmetro S_u sem a chave secreta. Uma chave de sessão é gerada toda vez que o usuário se autentica em um dispositivo para impedir o uso de antigos parâmetros em outros dispositivos

- Ataque MITM: a fim de proteger o sistema de este ataque, o ASs depois de receber a mensagem do dispositivo IED, envia um OTP por outro canal a fim de verificar a identidade, portanto para obter a chave de sessão e validar a identidade do dispositivo e servidor, o usuário tem que fazer operações com os valores contidos na mensagem recebida e com o OTP enviado pelo servidor.

- Ataques de Repetição e injeção: um atacante pode interceptar uma mensagem para executar um ataque de repetição, mas também pode injetar dados na mensagem. Para resistir este ataque, todas as mensagens tem um *timestamp*(t_i), por outro lado se tem valores aleatórios escolhidos para cada sessão como r, T, K_s e funções *hash* para verificar a integridade da mensagem.

- Ataques de redirecionamento: cada vez que um novo usuário tenta acessar um dispositivo, tem de fornecer informações de localização para o dispositivo. Posteriormente, se o mesmo usuário tenta fazer um segundo acesso o servidor verifica a sua localização por e compara com a localização da primeira sessão $L_1 =? L_2$, se são diferentes o servidor rechaça a segunda conexão.

- Ataques pelo pessoal interno: a autenticação dos clientes e o pessoal de manutenção é multifatorial o que contribui para segurança em caso de robô de credenciais, ademais os usuários só têm acesso de leitura apenas funções do papel atribuído, de modo que não pode extrair/modificar outras informações.

- Ataque de chave conhecida: o protocolo proposto é resistente a este ataque porque para cada sessão se tem uma chave diferente e para calcular a chave de sessão se precisa o OTP enviado ao usuário.

- Ataque de Repúdio: Um usuário só pode modificar o sistema somente após da autenticação e autorização de usuário, portanto, um usuário malicioso ou invasor não pode alterar os parâmetros de segurança do dispositivo.

- Ataques *DoS*: O Servidor permitirá que apenas o usuário validado acesse o dispositivo pois só um usuário válido pode enviar o parâmetro S_u certo, além disso, em caso de solicitar mais de uma sessão, o servidor verifica a localização de onde estão sendo enviadas as solicitações, em caso que existam diferenças entre as localizações (o sistema tem intervalo de localização aceitável) das solicitações enviadas pelo mesmo usuário o sistema rejeita a comunicação desse usuário para evitar até mesmo ataques DDoS.

Na Tabela 2 se mostra uma comparação resumida das propriedades de segurança do protocolo proposto e os trabalhos relacionados mencionados acima. Podemos dizer que algumas características estão presentes em todos os protocolos comparados: realizam autenticação mútua e acordo de chaves; usam chaves de sessão; ataques de repetição são evitados usando desafios, *timestamps* e números aleatórios durante autenticação; ataques *Man-in-the-Middle* são evitados, pois os parâmetros publicados no canal de comunicação não são suficientes para que um atacante gere mensagens e chaves de sessão válidas; todos conseguem se contrapor a ataques de personificação e repúdio.

Tabela 2. Análise de segurança dos protocolos.

	Vaidya 2013	Saxena 2016	Protocolo proposto
Autenticação Mútua e Acordo de Chaves	Sim	Sim	Sim
Confidencialidade	Sim	Sim	Sim
Integridade	Não	Sim	Sim
Privacidade	Sim	Sim	Sim
Ataques de injeção	Não	Sim	Sim
Resistência ao Ataque de Repetição	Sim	Sim	Sim
Ataques pelo pessoal interno	Sim	Sim	Sim
Ataque de chave conhecida	Não	Sim	Sim
Resistência ao Ataque <i>DoS</i>	Sim	Não	Sim
Resistência ao Ataque <i>Man-in-the-Middle</i>	Sim	Sim	Sim
Resistência ao Ataque de Redirecionamento	Não	Sim	Sim
Resistência ao Ataque de Personificação	Sim	Sim	Sim
Ataque de Repúdio	Sim	Sim	Sim

Verifica-se que o protocolo de [Vaidya 2013] não faz uso de funções Hash para garantir a integridade das mensagens trocadas no canal aberto, e não usa *timestamps* para resistir ataques de redirecionamento. Por outro lado, [Saxena 2016] não faz análise sobre como seu protocolo poderia resistir a ataques *DoS* na fase “Identity Creation”. Por tanto o protocolo proposto tem algumas vantagens de segurança com relação aos protocolos dos trabalhos relacionados.

5.2. Análise de Desempenho

Visto que este protocolo ainda não foi implementado só se avaliara o desempenho do protocolo de forma analítica, apresentando o custo de comunicações e o custo computacional do protocolo proposto e posteriormente se realizara uma comparação com os trabalhos mencionados neste trabalho.

d) Custo de Comunicações

O Custo de comunicação é o número total de bits transmitidos pela rede durante a execução do protocolo. Para calcular o custo de nosso protocolo se usara a mesma tabela de valores do trabalho de [Saxena 2016] que se mostra na Tabela 1. a fim de simplificar os cálculos e fazer uma adequada comparação com os outros trabalhos.

O protocolo proposto troca 4 mensagens, os custos de comunicação se mediram em *bits* os valores transmitidos mostra-se a seguir:

Mensagem 1:

$$S_u (128 \text{ bits}) + y_u (128 \text{ bits}) + L (32) + ID_{IED}(128 \text{ bits}), + t_1(64 \text{ bits}) + H_{m1}(128 \text{ bits}) = 608 \text{ bits}$$

Mensagem 2:

$$S_u (128 \text{ bits}) + y_u (128 \text{ bits}) + L (32) + ID_{IED}(128 \text{ bits}), + t_2(64 \text{ bits}) = 480 \text{ bits}$$

Mensagem 3:

$$Cert_u(128 \text{ bits}) + P_A(128 \text{ bits}) + Role(64 \text{ bits}) + T(3 \text{ bits}) + t_3(64 \text{ bits}) = 383 \text{ bits}$$

Mensagem 4:

$$\varphi(384 \text{ bits}) + X_1(128 \text{ bits}), X_2(128 \text{ bits}) + t_4(64 \text{ bits}) = 704 \text{ bits}$$

Em total o custo de comunicações para o protocolo proposto é 2175 *bits*, considerando um usuário. A seguir, se mostra a Tabela 3 onde se faz uma comparação dos custos computacionais dos protocolos. Com o fim de fazer uma comparação mais justa só se analisara o custo de comunicações na fase de acesso ao dispositivo.

Tabela 3. Comparação dos custos de comunicação com outros trabalhos.

	Vaidya - 2013	Saxena - 2016	Protocolo Proposto
Mensagem 1	384 <i>bits</i>	704 <i>bits</i>	608 <i>bits</i>
Mensagem 2	256 <i>bits</i>	768 <i>bits</i>	480 <i>bits</i>
Mensagem 3	64 <i>bits</i>	451 <i>bits</i>	383 <i>bits</i>
Mensagem 4	64 <i>bits</i>	704 <i>bits</i>	704 <i>bits</i>
Mensagem 5	128 <i>bits</i>	- 0 -	- 0 -
Mensagem 6	128 <i>bits</i>	- 0 -	- 0 -
Totais	1024 <i>bits</i>	2627 <i>bits</i>	2175 <i>bits</i>

A partir da Tabela 3 é possível concluir que o protocolo de [Vaidya 2013] tem o menor custo de comunicação quando comparado aos demais protocolos analisados, mas tem falhas graves de segurança na integridade das mensagens e de vulnerabilidades a

ataques de redirecionamento; além disso tem um numero mais alto de mensagens trocados que afetam seu desempenho. Note-se que o protocolo proposto fica no segundo lugar, mas tem melhores características de segurança entre os protocolos comparados.

e) Comparação de desempenho

A comparação do desempenho dos artigos será feito analiticamente, considerando as notações: Tempo de execução de função *hash* (H), Multiplicação Modular (M), Adição Modular (A), Emparelhamento Bilinear(P), Ciframento (E), Deciframento (D).

A comparação do custo computacional do protocolo proposto com os outros esquemas analisados é apresentada na Tabela 4. A operação *xor* foi omitida, pois é desprezível se comparada com outras.

Tabela 4. Comparação dos custos computacionais.

Trabalhos	ENTIDADES			Total
	MP ou UA	IDE/SM/OFE	AS ou SSC	
Saxena 2016	4M, 2H, 1D, 1P	6M, 5H, 1A, 1E	4M, 2H, 1A	14M, 9H, 1D, 1P, 2A, 1E
Vaidya 2013	3H, 4A, 4M	2H, 2A, 1M	2H, 3A, 5M	7H, 9A, 10M
Protocolo Proposto	4M, 4H, 1P, 1A	7M, 3H, 2A	2M, 1H	13M, 8H, 1P, 3A

Na Tabela 4 o protocolo proposto tem o menor custo computacional que [Saxena 2016], mas não que [Vaidya 2013] devido a que este não faz operações que ajudem a garantir a integridade das mensagens, além disso, não tem dobre fator de autorização para garantir a identidade do usuário em caso de difusão da chave secreta.

6. Conclusão e Trabalhos Futuros.

A construção de cidades inteligentes pode se beneficiar do desenvolvimento de sistemas como SG para melhorar a vida da população e otimizar os recursos territoriais, econômicos e ambientais, havendo problemas de segurança como os de autenticação e autorização a serem adequadamente resolvidos.

Neste trabalho foi apresentado um novo protocolo de autenticação e autorização de usuários em uma rede *Smart Grid*, com base em *Certificate-Based Signcription* (CBS) e em Emparelhamento Bilinear.

Quando comparado com dois outros protocolos, o protocolo proposto apresenta melhor atendimento a propriedades de segurança. Adicionalmente, seu custo computacional e de comunicações e inferior ao de [Saxena 2016], e maior que o protocolo proposto por [Vaidya 2013]. Todavia, este protocolo têm falhas graves de segurança que o protocolo proposto não tem.

Em resumo, o protocolo proposto cumpre com êxito seus objetivos. Ele apresenta excelentes resultados em relação a segurança e desempenho, provando-se como uma escolha segura e eficiente quando comparado a outros protocolos de autenticação e autorização para sistemas SG descritos neste trabalho.

Trabalhos futuros incluem a verificação formal da segurança do protocolo proposto com ferramentas como Avispa, Proverif e logica BAN.

Referências

- Kamienski, C., Biondi, G., Borelli, f., Heideker, A., Ratusznei, J., Kleinschmidt, J. (2016) “Computação Urbana: Tecnologias e Aplicações para Cidades Inteligentes”, XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos – Minicursos, cap 2, p. 51 – 100 .
- Lopes, T., Bornia, T., Farias, V., Fernandes N., and Muchaluat-Saade, D. (2016) “Desafios de Segurança e Confiabilidade na Comunicação para Smart Grids”, XXXIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - Minicursos, p. 142 – 186.
- Li, F., Xin, X. e Hu, Y. (2008) “Efficient Certificate – Based Singryption Scheme From Bilinear Pairings”, International Jurnal of Computers and Applications, v.30, No 2, 2008.
- R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, M. Guizani. (2011) “Cognitive Radio Based Hierarchical Communications Infrastructure for Smart Grid,” IEEE Network, vol.25, no.5, pp. 6-14.
- Coyne, E., Weil, T., (2013) "ABAC and RBAC - Scalable, Flexible, and Auditable Access Management", IT Professional, vol.15, Issue 3.
- Stallings, W (2014). “Cryptography and Network Security: Principles and Practice”, sixth ed. Boston: Pearson.
- Saxena, N., Choi, B., and Lu, B. (2016) “Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid”. IEEE Transactions On Information Forensics And Security. v.11, NO.5.
- Menezes, Alfred. (2005) “An Introduction to Pairing-Based Cryptography”, Recent Trends in Cryptography, v. 477, p. 47-65.
- Vaidya, B., Makrakis, D., and Mouftah, H. (2013) “Authentication and Authorization Mechanisms for Substation Automation in Smart Grid Netwok”. IEEE Network, v.27, P. 5-11.
- Brown, D., Campagna, M., and Vanstone, S. (2009) “Security of ECQV-Certified ECDSA Against Passive Adversaries”. Cryptology ePrint Archive, Report 620.
- Cheung, Herman., Yang, C., and Cheung, Helen. (2015) “New Smart-Grid Operation-Based Network Access Control” IEEE Energy Conversion Congress and Exposition P.1203 - 1207.
- Lee, B., Kim, D., Yang, H., and Jang, H. (2015) “Role-Based Access Control for Substation Automation Systems Using XACML”. Journal Information System, V.53, P.237 – 249.