Journal of Computer and Knowledge Engineering, VOL. 2, NO. 1, 2019.
DOI: 10.22067/cke.v2i1.74148

A Key Management Schema Based on ECC to Secure the Substation and Control Center Communications in Smart Grids

Mostafa Farhadi Moghadam[1*] Amirhossein Mohajerzdeh[2] Behzad Molavi [3]

Abstract: Since the invention of electricity, global power grids have been at the forefront of technological advances. The antiquated infrastructure of power system which provides power to the city's homes, factories and businesses are replaced with a new power distribution system. This new infrastructure of power distribution includes the collection of digital systems called the smart grid. In the smart grid, one of the main components is the distribution system, and the consumption reports are transferred from the substations to the control center. Currently, the smart substations use the IEC61850, however, it is not completely safe. IEC 62351 is used to secure this standard. However, the security protocols are provided for IEC 62351 standard, and there are different security issues to this standard. This paper presents a key agreement scheme with an authentication mechanism based on ECC for securing the communication between the data center and substation. In addition, it can cover the standard security weaknesses, and the session key is generated due to the time limit for the two important protocols in IEC 62851 (i.e. GOOSE and SV).

Key words: Session key, Authentication, Key agreement, Smart grids, Security, Substation

1. Introduction

As the next generation of power grids, the smart grid uses different smart devices used in different parts of the network, such as the electronic smart devices located at substation, programmable logic controller (PLC), remote terminal unit (RTU), smart meters in the home area network, and supervisory control and data acquisition (SCADA) system controlling the smart grid devices and outdoor equipment. The smart grid consists of 3 parts: control center, substations, and smart appliances. Substation is an important and intelligent part of the network; in fact, it is an integral and important part of the smart grid [5][6]. The communication between the substation and devices in the smart grid is necessary to keep it up to the operation in real time. At present, smart substations use the IEC 61850 standard for communications [1, 2 , 9], and most of the communications are reliant on Ethernet networks. The IEC (international electrotechnical commission) 61850 is an Ethernet-based communication standard (IEEE802.3) for power substations. The IEC 61850 is an open standard communication protocol; it can provide interoperability for hardware, but it cannot cover the security [3, 4]. In the smart grid, sensitive data are exchanged. Figure 1 illustrates the communication network architecture and the electricity distribution system in the smart grids.

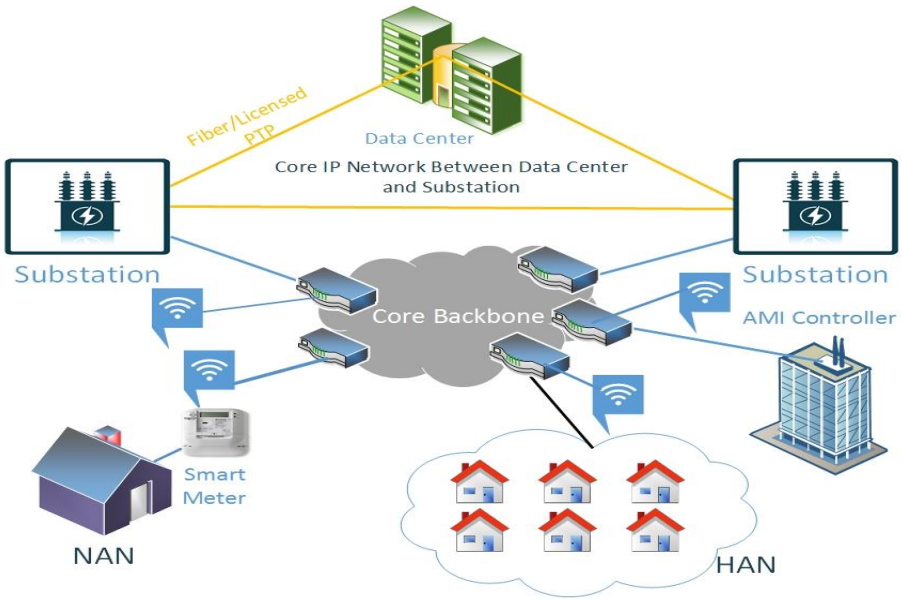

Fig.1. The communication network architecture and the electricity distribution system.

Manuscript received July. 15, 2018; accepted. September 30, 2018.
[1*] Ms student of Imam Raza international university, Iran, Mashhad, Email: Mostafa.farhadi@imamreza.ac.ir.
[2] Assistant professor, Department of Computer Engineering, Ferdowsi University of Mashhad .
[3] M. S.c Department of computer, Vahdat Institue of Higher Education,torbat-e Jam, Iran.

As the IEC 61850 does not consider cyber-security or secure communication, the IEC has published IEC 62351; this standard provides security for power system communication including cyber-security in the smart substation adapted with IEC 61850. The IEC 62351 consists of 11 parts; all of these parts are published except part 9 which addresses certificate and/or key management [7]. The IEC 62351 parts are explained as follow:

Part 1. This part of standard is the overview of the IEC 62351 standard; this part introduces the various aspects of information security, power systems management, and the associated information exchange, data and security communication network.

Part 2. The second part of the IEC 62351 standard includes access control, data security, and vocabulary used in many other parts of the standard.

Part 3. The third part of IEC 62351 addresses the security of TCP / IP (transmission control protocol/Internet protocol) based the protocols and the use of TLS (transport layer security) in the transport layer.

Part 4. This part of the IEC 62351 standard is for the security of profiles such as multimedia messaging service (MMS) and the use of authentication applications.

Part 5. The fifth part of this standard describes security for the protocols. These protocols are message-based and authentic. This part also proposes mechanisms for authentication and encryption

Part 6. This part of the IEC 62351 standard defines security issues for GOOSE/GSE (generic object oriented substation event/generic substation event) and SMV (sampled measurement values), which are the IEC 61850 protocols.

Part 7. This part of IEC 62351 describes object data models which are specific to power systems. In the smart grid, the power systems infrastructure uses the interconnected information systems to manage the operations.

Part 8. This part of the IEC 62351 standard defines the role-based access, certain mandatory rights and roles control for power systems infrastructure.

Part 9. This part of the standard has not been released yet, but it has been considered to address certificate and/or key management.

Part 10. This part provides general guidelines for the security architecture and an overview of security controls that can be applied in power systems.

Part 11. This part focuses on XML (extensible markup language) security. The XML-based substation control language are introduced by the standard IEC 61850. These files have to be protected. In this regard, some mechanisms such as XML signatures are used to protect these files. Table I summarizes the IEC 62351 standard parts.

Although security issues are considered in the IEC 62351, there are some weaknesses found in this standard, which are identified by the manual inspection of the protocol specifications [8]. These weaknesses are listed as follows:

A. Replay attack on the GOOSE protocol

In this protocol, when a legitimated message is sent, it can be used again after the stNum value is reset to zero. For this attack, the message that is used does not need to be changed.

B. Replay attack on the sampled values protocol

Another kind of replay attack occurs in this protocol. When a previously message is sent, it can be replayed to a different receiver. For this attack, malicious factors require two or more SV subscribers that are subscribed to the same data set of a logical node.

C. Attack on the SNTP (simple network time protocol)

To prevent the manipulation of the data in the IEC 62351 by the malicious factors, authentication schema are required. The RFC 1305 defines a message authentication code called MAC (message authentication code) over the SNTP package. This MAC uses the data encryption standard (DES) with a pre-shared symmetric key. This authentication schema has two problems: First, DES is not secured because the 56 bit keys are vulnerable to brute force attacks [10]. Second, DES is symmetric. In the RFC 1305, the same key can be used in a group of servers [11].

Table 1. The Overview of the IEC 62351 Parts

Parts	Titles
IEC 62351-1	Communication network and system Security: Introduction to security issues
IEC 62351-2	Glossary of terms
IEC 62351-3	Communication network and system Security: Profiles including TCP/IP
IEC 62351-4	Profiles including MMS
IEC 62351-5	Security for the IEC 60870-5 and derivatives
IEC 62351-6	Security for the IEC 61850
IEC 62351-7	Network and system management (NSM) Data object models
IEC 62351-8	Role-based access control
IEC 62351-9	Cyber security key management for power system equipment (unpublished)
IEC 62351-10	Security architecture guidelines
IEC 62351-11	Security for XML files

There are several protocols providing security and authentication for the smart grid; however, most of these methods are developed for smart meter communications. In this regard, there are limited works on the development of protocols used for substation communications, and most of them are not suitable for GOOSE and SV in the IEC 61850. In this paper, a security protocol with an authentication mechanism base on ECC is proposed that covers the IEC 62351 security vulnerabilities. To evaluate the protocol, tests are performed based on the type of cyber-attacks. In the communication between the data center and the substation there are two important protocols that they are in the IEC 62850 and exchange critical data. These protocols must transmit the messages within 4ms for real-time operation [24]. The main goal of the proposed scheme is to generate a session key based on the time limit for the protocols (i.e. GOOSE and SV) and the security of the data exchanged.

In the remainder of the paper, related work and protocols for secure communications in the smart grid are discussed in Section II. The proposed lightweight key management protocol is explained in Section III. Section IV lists the security analysis, and the evaluation results are described in Section V followed by the conclusion in Section VI.

2. Related Work

The smart grid is a network consisting of two parts: computer network and power infrastructure. This network is sensitive because of the data transmitted in it. When the sensitive and important data transmit in a network, the security issue becomes crucial to it. In recent years, many studies have been conducted on the smart grid security. Nicanfar et al. offered an efficient method to authenticate on a local area network which uses an initial password. In addition, they reduced the number of secure password protocol steps and exchange packages, and proposed an efficient key management protocol based on the encryption of self-authenticated authentication methods along with public key infrastructure [12]. Suhendray et al. proposed a security protocol; this protocol is used for providing secure communication, control and management in the smart grid. The proposed method specifically provides a key agreement and update protocol based on the symmetric key. The smart grid topologies can effectively identify and deny vulnerabilities through this proposed schema [13].

Abbasinezhad-Mood and Nikooghadam proposed an anonymous elliptic curve cryptography-based self-certified key distribution scheme. Their schema is efficient and it is free from the overhead of the certificate management and the key escrow issue. Furthermore, they implemented the cryptographic elements on two state-of-the-art ARM chips [14]. Alishahi et al. proposed a secure infrastructure for communication in a smart grid. They focused on two networks, namely HAN and NAN. They also proposed a key agreement scheme based on elliptic curve cryptography (ECC). The proposed scheme in the transmit message steps and the use of operators is cost-efficient [15]. Odelu et al. first analyzed the security of a recent relevant work in a smart grid and then proposed scheme which reduces the computation overheads and offers more security features [16]. He et al. proposed an anonymous key distribution (AKD) scheme based on the elliptic curve cryptography. The proposed AKD scheme provides the anonymity and mutual authentication between two entities without any help of the trust agent. They proposed AKD scheme better than the latest AKD schema [17]. Amoah et al. proposed a new lightweight security scheme for broadcast mode communication (DNP3 secure authentication for broadcast). The proposed scheme is based on hash chain which is integrated into the DNP3-SA key update process [18]. Tsai et al. proposed a new anonymous key distribution scheme for the smart grid environments using an identity-based signature and an identity-based encryption scheme. The proposed schema requires a few computation operations and service providers during the authentication using private key without the help of the trusted agent [19].A hybrid Diffie-Hellman based lightweight authentication scheme is proposed by K. Mahmood et al in 2016 [20]. This schema uses AES and RSA for session key generation. As integrity is another security parameter, in this protocol hash-based message authentication code is exploited. Other features provided by this protocol are mutual authentication, thwarting replay, man-in-the-middle attacks and achieves to the message integrity. He et at proposed an anonymous key distribution scheme that uses the elliptic curve cryptography proposed in 2016 [21]. The proposed scheme consists of three phases, including the system setup phase, the extraction phase, and the key distribution phase. The distributed network protocol version 3 (DNP3) is a standard for supervisory control and data acquisition (SCADA) systems and is designed to facilitate communications in smart grid automation. An update to the DNP3 protocol using Coloured Petri Nets (CPN) called DNP3-SA is proposed for security issues [22].

3. Proposed Schema

In the smart grid network infrastructure, the communication between the data center and the sub is considered to be dedicated [23] [24].However, we know that physical connection cannot provide security completely. In the network with dedicated communication infrastructure, if physical access to the network can be established by the attacker, the security of the network will be completely vulnerable. Given that the dedicated communication network infrastructure can be vulnerable, so in this section of the article we proposed scheme that provide secure communication between substation and data center. Furthermore, there are two important protocols in the IEC 61850 which are used in the network. These two protocols are generic object oriented substation event (GOOSE) and sample values (SV) [25]. These protocols are used to broadcast multimedia messages and switch Ethernet network to communicate [26] [27]. They must also transmit the messages within 4ms in real-time operation [27].

The proposed scheme consists of two phases: *registration phase* and *key agreement phase*. In the first phase, the substation and data center exchange parameters which are carried out in a secure channel. In the key agreement phase, the data center and substation authenticate each other and

compute session key based on the ECC. Table 2 describes the protocol symbols below:

Table 2. Symbols Used in the Proposed Protocol

Symbol	*Definition*
PU_{sub}	The public key of substation
K_{sub}	The private key of substation
PU_{dc}	The public key of data center
K_{dc}	The private key of data center
E_k	symmetric key
Cert	The certificate of substation
H	One-way hash function
ΔT_i	The time of sending a packet
P,M1,M2	Messages
SK	Session key

A. Registration Phase

In the registration phase, substation sends ID and PU parameters to the data center. Next, the data center receives parameters which are sanded by substation. This generates a special certificate for substation. For generating certificate, there are various generation/ authentication algorithms that can be used. The data center can authenticate each of the substation by their generated certificate. In the final step of this phase, the data center chooses a particular symmetric key to encrypt the messages sent in communication and then sends it along with certificate to the substation. Fig 2 shows the registration phase of the proposed schema.

B. Key agreement Phase

The proposed schema in this phase performs two important operations in two handshake authentications and compute the session key. The steps in this phase are as follows:

1. The substation chooses from random natural numbers and then generates parameter P, M1 and sends them to the data center.

$P=H(Cert\|ID_{sub})$ and $M1=H(P||T_i||PU_{sub}||a)$

Parameter P in message M1 helps the data center for authenticating the substation.

Next, these parameters are encrypted by the symmetric key which chooses the data center in the registration phase and send to the data center.

2. When the data center receives the message from the substation, first it checks message freshness by checking the ΔT, and then computes $P'=H(Cert \text{ ll } ID_{sub})$ for authenticating the substation. If Parameter $P'=P$, then the Data center accept the request of the substation. After confirming the value of parameter P´, the Data center compute rhe session key base on the ECC and generate parameter M2:
   $SK=H(D_{dc}.PU_{sub}||M1)$, $M2=H(SL||T_i||P)$
   Parameter M2 encrypted by the symmetric key and the message sent to the substation.
3. In the final step of key agreement phase, the substation receive the message that sent by Data center. Data center encrypt the message by Public key of the substation and Substation to access the message must decrypted it by its own private key. After the decryption, substation first check the ΔT to check the freshness of message. second, compute P´ to ensure the authenticity of the message sent by the data center. Finally,substation compute paramters SK´ and M2´ as follow:

$SK'=H(K_{sub}.PU_{dc}||M1)$, $M2'=H(SK'||T_i||P)$

If M2´=M2 substation chooses the SK´ as the session key. In addition, the proposed schema investigates authentication using the two parameters of P and SK while they are generated by two entities based on the ECC. Fig 3 shows the key agreement phase of the proposed schema below:

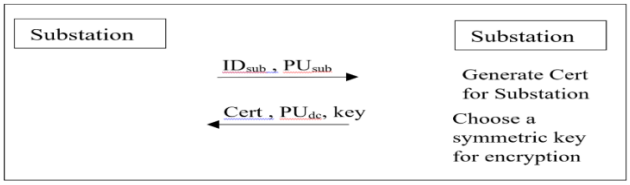

Fig. 2. Registration phase

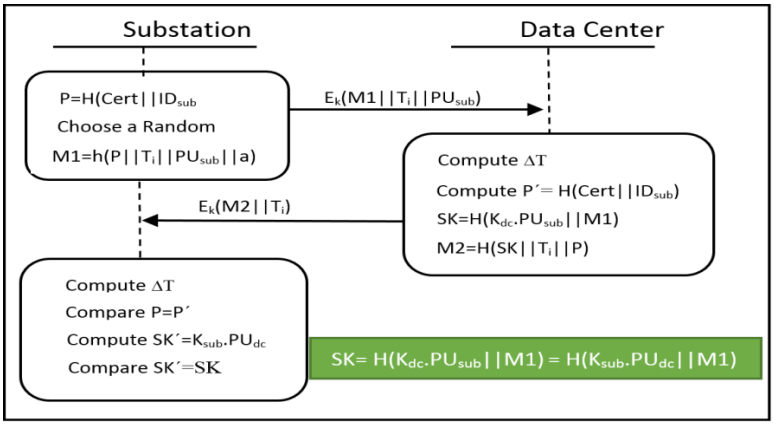

Fig. 3. Key agreement phase

4. Security Analysis

1. Reply attack

A replay attack is a category of network attack in which an attacker detects a data transmission and fraudulently has it delayed or repeated. During replay attacks, the intruder sends the victim the same message as was already used in the victim's communication. The message is encrypted, so its receiver may treat is as a correct request and takes the actions desired by the intruder. The proposed schema to prevent this type of attack use Timestamp and check message freshness. For example, the attacker sends the $E_k(M1||T_i||PU_{sub})$, the data center then checks ΔT and if it is not fresh, the data center will reject the connection. Meanwhile, the message is encrypted by the symmetric key; therefore, the attacker cannot access the details of the message.

2. Perfect forward secrecy

The perfect forward secrecy is a method that helps protocols create different session key in each session. In other words, in communication a totally different secret key is encrypted between two entities each session, while the session keys are not related. In the proposed schema, M1 is used to create the session key, which is different in each session; therefore, the session key for any substation in each session will be different.

3. Man-in-the-middle attacks (MITM)

A MITM attack happens when a communication between two systems is intercepted by an outside entity. In this protocol if the attacker intercepts the connection between the substation and the data center, he/she cannot access the message data because the data are encrypted by the symmetric key.

4. Impersonation attack

Impersonation attack is a type of attack which an adversary successfully assumes the identity of one of the legitimate parties in the system or in a communication protocol. In the communication between substation and data center if the attacker wants to introduce himself/herself as an authorized substation he/she needed to parameters Cert, P and M1,But as described in the key agreement section, parameter Cert for the data center is a private parameter and also has an effect on the production of value When the substation message is received by the data center, the data center re-calculates the value of P to verify authentication, and this value is generated by the authorized certificate generated by the data center for each substation. Therefore, the attacker cannot identify himself/herself as an authorized substation. Also, before generating session key in both side, proposed protocol used the authentication method depended on the private and public key.

5. Preserve mutual authentication

Preserving mutual authentication points out that two entities must authenticate each other before generating the session key and exchanging the parameters. In the proposed method, entities' authentication is performed in two steps. In the first step, the data center authenticates the substation by re-computing the parameter p, whereas the two entities authenticate each other while generating the session key base on the ECC in the second step.

6. Untraceability attack

In this type of attack, the adversary has access two messages from two different sessions and compares them. If these two messages are generated from the same parameters, he\she understands that these messages were sent by an identical entity. In the proposed protocol, M1 and M2 values are related to P and T_i ; in fact, these parameters are completely different in each session, because to generating the parameter P used a random number and timestamp. These parameters make difference value for session key in each session.

5. Result and Analysis

AVISPA result OFMC and ATSE

AVISPA (automated validation of Internet security protocols and applications) is a automatically verifying and analyzing tool for the Internet security protocols; it is one of the most trusted evaluation tools that analyzes security and the capability of the security protocols to withstand various attacks. This tool provides two types of output called *integrated automated security analysis* and *back-end servers*, such as the Onthe-Fly Modeler (OFMC) and analyst and constraint-logic (Cl-AtSe) attacker. This part of the paper investigates the security of the proposed protocols implemented by the AVISPA tool. Fig 4 demonstrates the results of the analysis below:

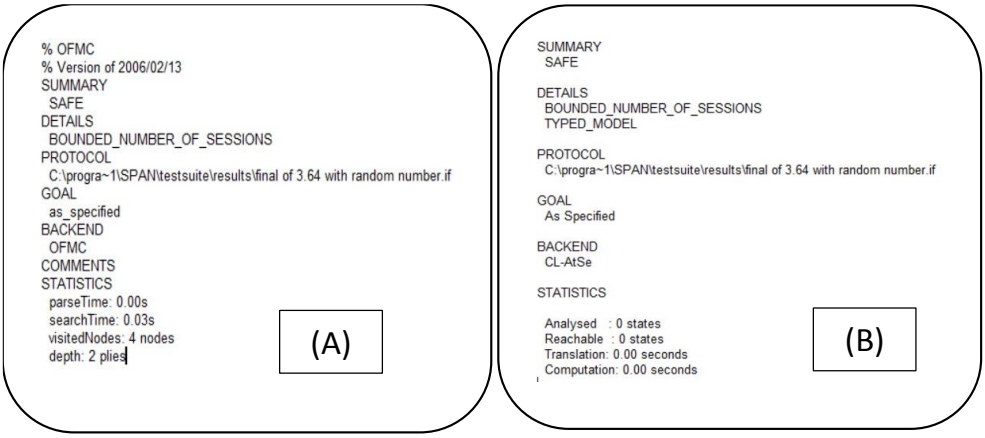

Fig. 4. AVISPA results: (A) OFMC, (B) ATSE

According to Figure 4, the proposed schema can be safe against a variety of attacks. The OFMC and CL-ATSE output show the confidentiality of the private parameters and the messages exchanged between the two entities are retained. Furthermore, it is safe against the active and non-active types of attacks. As stated in the proposed scheme section, GOOSE and SV protocols are used to broadcast multimedia messages across the LAN, and they use switched Ethernet network. These protocols are needed to transmit the messages within 4ms in the real time operations. Due to the time limit for the two protocols GOOSE and SV, in the proposed protocol the two entities agree on the session key less than 4 Ms. In this section, time efficiency of the proposed protocol is examined. Because the data center and the resource base are not limited, a system with 3 GHz Pentium IV is considered. The calculation time of the operations used in the protocol is presented in Table 3 [28].

Table 3. Computation Time of Cryptographic Operations

Operation	Pentium IV 3GHz
Hash Function	~0ms
AES Encryption/Decryption	~0ms
Point Multiplication	1.82ms

According to the time cost table and the proposed protocol, the time consumed of the key agreement phase for the two entities is 3.64 milliseconds. Therefore, the substation and the data center can achieve the session key at the right time. As mentioned in Table 3, the proposed protocol can generate the session key in less than 4 Ms. This protocol can satisfy the time constraints for the protocols GOOSE and SV. In addition, since the session key for communication between each substation and data center and the session key of the past sessions are completely different, the proposed schema can resolve the shared key problem in communications which are based on the IEC 62351.

6. Conclusion

This paper first introduces the smart grid and the infrastructure of the substation and the data center communication with their communication protocols. Then, it investigates some security weakness in the communication protocols used in the smart grid. In addition, the two protocols of GOOSE and SV and the time needed to exchange information via them is described. According to the described conditions, highly sensitive data exchanged in communications and there is the time limit in the communication protocols. This paper aims to propose a secure protocol to generate a session key for the communication between the substation and the data center through an authentication mechanism base on the ECC. Finally, the paper analyzes the security of the proposed protocol using the AVISPA tool.

APPENDIX IMPLEMENTATION OF THE PROPOSED MECHANISM IN AVISPA

The AVISPA tool provides a set of applications which can be used for building and analyzing the formal models of security protocols. High level protocol specification language or HLPSL is used to write the protocol models in this tool. In this section, the HPLSL codes for the substation and data center roles called SUB and DC roles are presented. Fig 5 and 6 show the sub and Dc roles codes. The codes for session and environment roles are also presented in Figure 7.

```
role sub(Sub,Dc:agent,
H,Mul,Add:hash_func,
Snd,Rcv:channel(dy))
played_by Sub
def=
local State:nat,
PUsub,PUdc:public_key,
Kds,Ksub,Kdc:symmetric_key,
Cert,IDsub,T1,Pi,T2,SK,Ai,M1,M2:text,
Inc:hash_func
const sub_dc_T1,sub_dc_M1,sub_dc_Ai,dc_sub_T2,dc_sub_M2,dc_sub_sk,
sub1,sub2,sub3:protocol_id
init State:=0
transition
1.State=0 /\ Rcv(start) =|>
State':=1  /\ Pi':=H(Cert. IDsub)
/\ T1':=new()
/\ Ai':=new()
/\ M1':=H(Pi.T1.Ai)
/\ Snd ({T1'.M1'}_Kds)
/\ secret({M1,T1,Ai},sub1,{Sub})
/\ secret({M1,T1},sub2,{Dc})
2.State=1 /\ Rcv({T2'.M2'}_Kds)=|>
State':=2
/\ request(Dc,Sub,sub_dc_M1,M1')
/\ secret({T2',M2' },sub3,{Sub})
/\ secret({T2',M2' },sub2,{Dc})
/\  Rcv({M2'.T2'}_Kds)
/\ secret({T2',M2' },sub3,{Sub})
/\ request(Sub,Dc,dc_sub_M2,M2')
/\ SK':=Ksub.PUdc
end role
```

Fig. 5. HLPSL code for role sub.

```
role dc(Sub,Dc:agent,
H,Mul,Add:hash_func,
Snd,Rcv:channel(dy))
played_by Dc
def=
local State:nat,
PUsub,PUdc:public_key,
Kds,Ksub,Kdc:symmetric_key,
Cert,IDsub,T1,Pi,T2,SK,M1,M2:text,
Inc:hash_func
const sub_dc_T1,sub_dc_M1,sub_dc_Ai,dc_sub_T2,dc_sub_M2,dc_sub_sk,
sub1,sub2,sub3:protocol_id
init State:=0
transition
1. State = 0 /\ Rcv({T1.M1}_Kds) =|>
State' := 1
/\ SK':=Kdc.PUsub
/\ T2':=new()
/\ M2':=H(SK'.T2')
/\ Snd({T2'.M2'}_Kds)
/\ secret({Cert,M1,Pi},sub1,{Sub})
/\ secret({Kdc},sub2,{Dc}) %%%/\ secret({Pi,M1,Kdc},sub2,{Dc})
/\ secret({T2',Pi',M2'},sub2,{Dc})
/\ secret({T2',M2' },sub3,{Sub})
/\ witness(Dc,Sub,dc_sub_M2,M2')
end role
```

Fig. 6. HLPSL code for role Dc.

```
role session(Sub,Dc:agent,
H,Add,Mul:hash_func)
def=
local SI,SJ,RI,RJ:channel(dy)
composition
sub(Sub,Dc,H,Add,Mul,SI,RI)
/\ dc(Sub,Dc,H,Add,Mul,SJ,RJ)
end role
role environment()
def=
        const sub,dc:agent,
        h,add,mul:hash_func,
        sub_Dc_M2,
        sub1,sub2,sub3:protocol_id,
        idsub,t1,pusub,pudc:text

intruder_knowledge={sub,dc,idsub,t1,pusub,pudc,h,add,mul}
composition
session(sub,dc,h,add,mul)
/\ session(sub,dc,h,add,mul)
end role
goal
secrecy_of sub1
secrecy_of sub2
secrecy_of sub3
authentication_on  sub_dc_Ai
authentication_on  dc_sub_sk
authentication_on  sub_dc_M1
authentication_on  dc_sub_M2
end goal
environment()
```

Fig.7. AVISPA session and environment HLPSL codes.

References

[1] Q. Song, W. Sheng, L. Kou, D. Zhao, Z. Wu, and H. Fang, "Smart substation integration technology and its application in distribution power grid," *CSEE Journal of Power and Energy Systems*, vol. 2, no. 4, pp. 31-36, 2016.

[2] E. Tebekaemi and D. Wijesekera, "Designing an IEC 61850 based power distribution substation simulation/emulation testbed for cyber-physical security studies," in Proceedings of the First International Conference on Cyber-Technologies and Cyber-Systems, pp. 41-49, 2016.

[3] C. Wester, M. Adamiak, and J. Vico, "IEC61850 protocol-practical applications in industrial facilities," in Industry Applications Society Annual Meeting (IAS), IEEE,pp. 1-7: IEEE, 2011.

[4] R. Tawde, A. Nivangune, and M. Sankhe, "Cyber security in smart grid SCADA automation systems," in Innovations in Information, Embedded and Communication Systems (ICIIECS), International Conference on, 2015, pp. 1-5: IEEE, 2015.

[5] L. Zhang, S. Tang, Y. Jiang, and Z. Ma, "Robust and efficient authentication protocol based on elliptic curve cryptography for smart grids," in Green Computing and Communications (GreenCom), *IEEE and Internet of Things (iThings/CPSCom)*, IEEE International Conference on and IEEE Cyber, Physical and Social Computing, pp. 2089-2093: IEEE, 2013.

[6] J. Northcote-Green, R. G. Wilson, "Control and automation of electrical power distribution systems". CRC Press, 2006.

[7] K. C. Ruland, J. Sassmannshausen, K. Waedt, and N. Zivic, "Smart grid security–an overview of standards and guidelines," *e & i Elektrotechnik und Informationstechnik*, vol. 134, no. 1, pp. 19-25, 2017.

[8] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in IEC 62351 protected Smart Grid control systems," in Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on, pp. 266-270: IEEE, 2016.

[9] Miao, Jianqiang, Ning Zhang, Chongqing Kang, Jianxiao Wang, Yi Wang, and Qing Xia. "Steady-state power flow model of energy router embedded AC network and its application in optimizing power system operation." IEEE Transactions on Smart Grid 9, no. 5, 4828-4837, 2017.

[10] T. Güneysu, T. Kasper, M. Novotný, C. Paar, and A. Rupp, "Cryptanalysis with COPACOBANA," IEEE Transactions on Computers, no. 11, pp. 1498-1513, 2008.

[11] David L. Mills. Network Time Protocol (Version 3) Specification, Implementation and Analysis. Internet Request for Comments, March, RFC 1305, 1992.

[12] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Systems Journal*, vol. 8, no. 2, pp. 629-640, 2014.

[13] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Prob. Control and Inf. Theory*, vol. 15, no. 2, pp. 159-166, 1986.

[14] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 7996-8004, 2018.

[15] M. Alishahi, M. Farhadi, S. Jafari, M. Taghavi, H. Moosavi, and A. Mohajerzadeh, "An efficient and light asymmetric cryptography to secure communication in smart grid," in 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE), pp. 248-252: IEEE, 2017.

[16] Odelu, Vanga, Ashok Kumar Das, Mohammad Wazid, and Mauro Conti. "Provably secure authenticated key agreement scheme for smart grid." IEEE Transactions on Smart Grid 9, no. 3. 1900-1910. 2016.

[17] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Communications*, vol. 10, no. 14, pp. 1795-1802, 2016.

[18] R. Amoah, S. Camtepe, and E. Foo, "Securing DNP3 broadcast communications in SCADA systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1474-1485, 2016.

[19] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906-914, 2016.

[20] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, "A lightweight message authentication scheme for Smart Grid communications in power sector," *Computers and Electrical Engineering*, vol. 52, pp. 114-124, 2016.

[21] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Communications*, vol. 10, no. 14, pp. 1795-1802, 2016.

[22] R. Amoah, S. Camtepe, and E. Foo, "Securing DNP3 broadcast communications in SCADA systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1474-1485, 2016.

[23] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Authentication and authorization mechanisms for substation automation in smart grid network," *IEEE Network*, vol. 27, no. 1, pp. 5-11, 2013.

[24] K. G. Nagananda and P. Khargonekar, "An approximately optimal algorithm for scheduling Phasor data transmissions in smart grid networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1649-1657, 2017.

[25] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, "A review of security attacks on IEC61850 substation automation system network," in Information Technology and Multimedia (ICIMU), *International Conference on*, pp. 5-10: IEEE, 2014.

[26] C. Kriger, S. Behardien, and J.-C. Retonda-Modiya, "A detailed analysis of the GOOSE message structure in an IEC 61850 standard-based substation automation system," *International Journal of Computers Communications & Control*, vol. 8, no. 5, pp. 708-721, 2013.

[27] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in Globecom Workshops (GC Wkshps), IEEE, pp. 1508-1513: 2012.

[28] Mohammadali, Amin, Mohammad Sayad Haghighi, Mohammad Hesam Tadayon, and Alireza Mohammadi-Nodooshan. "A novel identity-based key establishment method for advanced metering infrastructure in smart grid." *IEEE Transactions on Smart Grid 9*, no. 4. 2834-2842, 2016.