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

Mostafa Farhadi Moghadam1* Amirhossein Mohajerzdeh2 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 Institute 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

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(unpublished)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

Abbasi and NIKOOGHADAM proposed an anonymous elliptic curve cryptography-based self-certified key distribution scheme. Their scheme is efficient and 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 and achieves to the message integrity. He et al. 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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PU_{sub}</td>
<td>The public key of substation</td>
</tr>
<tr>
<td>K_{sub}</td>
<td>The private key of substation</td>
</tr>
<tr>
<td>PU_{dc}</td>
<td>The public key of data center</td>
</tr>
<tr>
<td>K_{dc}</td>
<td>The private key of data center</td>
</tr>
<tr>
<td>E</td>
<td>Symmetric key</td>
</tr>
<tr>
<td>Cert</td>
<td>The certificate of substation</td>
</tr>
<tr>
<td>H</td>
<td>One-way hash function</td>
</tr>
<tr>
<td>∆T_{i}</td>
<td>The time of sending a packet</td>
</tr>
<tr>
<td>P,M_{1},M_{2}</td>
<td>Messages</td>
</tr>
<tr>
<td>SK</td>
<td>Session key</td>
</tr>
</tbody>
</table>

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, M_{1} and sends them to the data center.

   P=H(Cert||ID_{sub}) and M_{1}=H(P||T_{i}||PU_{sub}||a)

   Parameter P in message M_{1} 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 ∆T, and then computes P'\neq H(Cert||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 the session key base on the ECC and generate parameter M_{2}:

   SK=H(D_{dc}.PU_{sub}||M_{1}) M_{2}=H(SL||T_{i}||P)

   Parameter M_{2} 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 ∆T to check the freshness of message. second, compute P' to ensure the authenticity of the message sent by the data center. Finally, substation compute parameters SK' and M_{2}' as follow:

   SK'=H(K_{sub}.PU_{dc}||M_{1}), M_{2}'=H(SK'||T_{i}||P)

   If M_{2}'=M_{2} 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:
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 it 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 Eq(M1||T||PU_sub), the data center then checks ∆T 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 substitution 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 substations 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 substitution and data center if the attacker wants to introduce himself/herself as an authorized substations 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 substitution 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 to 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; 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:

![AVISPA results: (A) OFMC, (B) ATSE](image-url)
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].

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.

Fig. 5. HLPSL code for role sub.
Fig. 6. HLPSL code for role Dc.

Fig. 7. AVISPA session and environment HLPSL codes.

References


