Preventing Cyber Attacks Against Smart Grids Using UTM Devices With A Mutual Efficient Authentication Protocol

[1] Fattaneh Pasand; [2] Ali Marjanian

[1] Department of Engineering Computer, Islamic Azad University, Bushehr
Bushehr, Iran

[2] Department of Engineering Computer, Islamic Azad University, Bushehr
Bushehr, Iran

Abstract—Smart grids are bilateral interconnected networks in which, data and information play a crucial role in the process of energy distribution. Thus, according to increasing development and complexity, they are mentioned as the cyber-physical systems. Obviously, the security and economic situation of countries are largely dependent on performance stability and safety of these systems. According to the high dependence of the smart grids to measurement sensors and communication technologies, these networks are very vulnerable to cyber attacks. Load reduction (LR) attacks that lead to false data injection (FDI) on Advanced Metering Infrastructure (AMI) sensors and produce the misleading operational decision of the power system are too important among all cyber attacks. So we proposed an efficient authentication protocol with identity protection for smart grids based on elliptic curve cryptography in which the substations and smart appliances realized mutual authentication and key agreement via a tamper-resistant smart card so that the adversary cannot obtain the real identities of them. As a result, the attacker cannot begin a cyber attack with impersonation and false data injection.

Keywords—*smart grids; cyber attacks; load reduction (LR) attack; Unified Threat Management (UTM); mutual authentication protocol*

1. Introduction

LR attacks can lead to immediate or delayed damage in power system operation. False data injection attacks can manipulate the estimations situation without detecting by corrective measure systems. In other words, the adversaries can change and damage the measured data by the RTU's, heterogeneous communication networks and LAN's control center. To prevent the attackers, such that they would not be able to begin an LR attack with impersonation and false data injection, we proposed an authentication protocol for smart grids in which the substations and appliances realized mutual authentication and key agreement via a tamper resistant smart card, so that the attacker cannot obtain the real identities of them.

Over the last ten years, several authentication protocols have been proposed to protect the data transmission. In an attempt to prevent the attacker from obtaining the habit of the customer through analyzing the power usage pattern, Chim et al. [3] designed an authentication protocol by using a tamper-resistant device at the appliance and a pseudo-identity for the smart grid network to protect the privacy of the customer. However, their protocol was suffered from impersonation attacks. Since only substations could authenticate appliances, the attacker could impersonate the substations to cheat the smart appliances. Furthermore, their protocol failed to provide a key agreement function capable of protecting the communication between smart appliances and substations. Besides, the clock synchronization problem could not be avoided, since a timestamp is used in the signing module of their protocol. Mostafa et al. [4] proposed a message authentication mechanism to reduce the computational cost by using the Computational Diffie-Hellman assumption for smart grids. In their protocol, key agreement and mutual authentication were realized by using Diffie-Hellman key exchange protocol between the smart meters distributed at different networks of the smart grid system. However, the computational costs of these two protocols were still very high due to the usage of expensive exponential operations [5]. In 2016, Zhang et al. [5] proposed an elliptic curve cryptography-based authentication with identity protection which is complete and suitable for smart grids. Our protocol is similar to Zhang et al. [5] protocol, but with less storage overhead. Qing et al. [6] designed a multicast authentication protocol for smart grids by using a one-time signature to reduce the signature size and the storage cost. Because the one-time signature-based multicast authentication could provide low computation cost and short authentication delay, their protocol achieved a suitable performance. However, they only focused on designing a light-weight protocol, and the key agreement issue remains unsolved. Soohyun Oh et al. [7] proposed key establishment and a mutual authentication based on PKCs to strengthen the security of smart grid communications. In their protocol, the pre-shared long-term key and data concentration unit's PKC were used to realize the authentication between the intelligent devices and the data concentration unit. But the problem of distributing the shared key limited this protocol's applicability and scalability. In [10] a biometric technique for smart grids was also adopted to achieve strong authentication. Due to the use of biometrics, these protocols are very complex. Binod Vaidya et al. [13] suggested an authorization and authentication mechanism for smart grid networks. They realized attribute-based authorization and multi-factor authentication in a smart grid environment by using PKCs, access control and zero-knowledge technologies. But the heavy computational load could not be avoided since the implement of the public key cryptography calculation and PKCs management. Nicanfar et al. [15] proposed a password authenticated group key agreement protocol for a smart grid.

Although their protocol enhanced the security of communications and provided backward and forward secrecy, the usage of expensive exponential operations decreased the practical application of it. Nicanfar et al. [17] suggested a password-authenticated key exchange based on ECC to reduce the computational cost. This protocol is more efficient according to the usage of Elliptic Curve Cryptography, but a password needs to preload between the HAN controller and a smart appliance, which may arouse an intractable problem of password table maintenance and make this solution hard to scale. Li et al. suggested fault-diagnosable authentication architecture for advanced metering infrastructure [19], but in their authentication mechanism, key negotiation is not considered.

Considering the above description, protocol [3] is vulnerable to impersonating attacks and protocols [4, 6-19] were suffered from eavesdropping since these protocols could not provide key agreement. These protocols could not provide security at an acceptable level, although some of them achieved good performance. Therefore, other than Zhang et al.'s protocol [5], all the other mentioned protocols are not suitable for the smart grid. In this paper, we suggested an authentication protocol based on ECC with identity protection for smart grids by using tamper-resistant smart card security features. Our protocol has two phase, initialization phase and authentication phase which we will illustrate them in details. After that, we will show the completeness of proposed protocol by GNY logic [22], and finally, we will finish by some recommendations and conclusion.

2. The Security Requirements for Dealing With Cyber Attacks

In general applications of the network, because of data exchange in a public space such as Internet, there are many security risks. However, the general protocols, such as HTTP and FTP that exchange information based on the TCP/IP protocol, have designed without important security considerations, thus transmitted information can be easily intercepted or manipulated within the network.

We can use the lower layer of the network, including the following sections:

- The user workstations
- The application and infrastructure servers
- The public servers

Typically a firewall or a comprehensive UTM is located at the gateway and protect the network against external threats. Users can log in to the network with connecting to the UTM system.

To prevent cyber attacks, these devices should have the following security services.

- User authentication to the servers
- Server authentication to the users
- Access Control
- Tracking user activity
- Non-repudiation
- Confidentiality of data exchanged
- Integrity of the exchanged data and messages
- Prevention of unauthorized users
- Prevention of malicious code and false data injection
- prevention of internal intruders

3. Security establishment with UTM

In general, we can divide the smart grid network into three levels: control center, substations, and smart appliances. The SCADA system is used to protect the communications between the substations and the control center [1], but the other two levels need some security solutions [2].

There are a lot of security solutions for network applications that each of them provides some of the required security services. An important way to protect the network against external threats is using the UTM systems.

Major security services that provided by UTM devices are:

- Stateful firewall

- Virtual private network (VPN) with IPSec and PPTP protocols
- Authentication of users accessing the Internet (locally or connect with Active Directory)
- The possibility of grouping users and define different security policies for each group.
- Define different policies to access the network
- Virus detection and filtering Web traffic
- Caching
- Intrusion Detection System
- Bandwidth management

Therefore, we can use UTM systems in substations to prevent a lot of threats and attacks. In smart grid, the power DSO uses real-time measurement data from the AMI for accurate, efficient, and advanced control and monitoring. Smart grids are vulnerable to cyber attacks like the FDI attack on the Advanced Metering Infrastructure sensors that produce the misleading operational decision of the power system [26]. We can use an Intrusion Detection framework based on consumption pattern of the end-users in UTM systems to protect AMI. Our focus is on the communication security between substations and smart appliances, and we will propose an authentication protocol which will be used in UTM systems.

4. Our Proposed Authentication Scheme

Since ECC based on elliptic curve discrete logarithm problem can be implemented in different ways rather than a single encryption algorithm and it is more Complex than Integer factorization problem and discrete logarithm problem and also uses smaller key size and has more computational efficiency, we proposed our scheme based on it for smart grids. Considering the efficiency, we will use Elliptic Curve Cryptosystem version for El-Gamal public key encryption in our protocol where the cycle group is taken from elliptic-curve. For more details, please see [24]. There are two phases in our protocol, and the procedure of them is described in detail as follows.

A. Initialization phase

Security parameters used for key agreement and authentication are calculated by the substations and the control center according to the following steps.

1) The control center chooses an elliptic curve $E_p(a,b)$: $y^2 = x^3 + ax + b \pmod p$ over F_p and a base point P over this equation, where $a,b \in F_p$. Then, the control center writes P to the smart card memory TR_i and the substations.

2) The control center allocates an identity $TRID_i$ for each smart appliance TR_i and preloads them into the memory of the corresponding smart card. Then the identity $TRID_i$ is written in an ID table by the control center. Then, the control center submits the identity table to the substation over a secure channel and assigns an identity $SSID_j$ for each substation SS_j. The substation SS_j stores the identity $SSID_j$ in its memory securely. These identities should be unique to avoid reflective attacks.

3) The substation chooses a random integer $s \in Z_p{}^*$ as a secret key for symmetric cryptography and generates a random integer $k_{pr} < n$ as a private key and computes its corresponding public key $k_{pu} = k_{pr}P$, where n is the order of the base point P. The computed key pair (k_{pu}, k_{pr}) will use for asymmetric cryptography. Then the substation calculates $SEC = (E_s(TRID_i) \parallel SSID_jP)$ for every smart appliance TR_i. Since the protocol uses each of the two sections of the SEC sequence separately, we named every part of it as follow:
$SEC_1 = E_s(TRID_i)$ and $SEC_2 = SSID_jP$

As a result, SEC_1 is a 32 bits sequence to transform the main identifier of a smart card into a 32 bits anonymous identifier with symmetric encryption. Also, SEC_2 is a 1024 bits sequence which is a point on chosen elliptic curve and an anonymous identifier for substation j.

The system keys and the key pair (k_{pu}, k_{pr}) are kept secret by the substation. Furthermore, the substation writes the public key k_{pu} and the secret sequence SEC into each corresponding tamper-resistant smart card. If a new smart appliance TR_j wants to incorporate into the smart grid, the substation and the control center should cooperate to accomplish the initialization of the new smart appliance. The control center will allocate a new identity $TRID_j$ for TR_j and will record it in the ID table. Then, over a secure channel, it will send the identity of the new appliance to the related substation. The substation will record the identity in its ID table and then computes a secret SEC for the new appliance. Eventually, the substation writes the identity $TRID_j$, the point P, the public key k_{pu} and the secret sequence SEC into the tamper-resistant smart card of TR_j to achieve the initialization of the new appliance.

B. Authentication phase

The substation and the smart appliance TR_i, during the authentication process, perform the following steps to realize mutual authentication and key agreement.

1) First, the tamper-resistant smart card of TR_i selects an integer $rand_1 \in_R Z_p{}^*$ randomly to compute
$M_1 = e_{kpu}(TRID_i \| SEC_1 \| rand_1)$, where $e_{kpu}(\bullet)$ denotes the public key encryption function using the substation

SS_j's public key k_{pu} and $SEC_1 = E_s(TRID_i)$ is the first part of the secret stored in the tamper-resistant smart card of TR_i. Then, TR_i sends M_1 to the substation SS_j.

2) The substation SS_j obtains $TRID_i$, SEC_1, and $rand_1$ by decrypting the receiving message M_1 via its private key k_{pr}. Then, it checks whether $TRID_i$ is valid by matching it in the ID table. If not valid, the authentication process stops. Otherwise, the substation SS_j uses the system keys to decrypt SEC_1 and then gets the $TRID_i$. Next, it compares the value of $TRID_i$ in M_1 with that of $TRID_i$ in decrypted message SEC_1. If they are not equivalent, the authentication process terminates by the substation; otherwise, two random integers $rand_2 \in Z_p{}^*$ and $rand_3 \in Z_p{}^*$ chooses by the substation to calculate the shared session key $SK = rand_1 \oplus rand_2$ and authentication message $M_2 = E_{rand1}(SSID_j \| rand_2)$, where $E_{rand1}(\bullet)$ denotes the symmetric encryption algorithm with the secret key $rand_1$. Eventually, the substation SS_j submits the message $(M_2, rand_3)$ to TR_i.

3) After receiving the message $(M_2, rand_3)$, the smart appliance TR_i adopts $rand_1$ to decrypt M_2 and then obtains $rand_2$ and $SSID_j$. Then it calculates $SSID_jP$ and checks whether the following equation holds $SEC_2 = SSID_jP$. If the equation holds, it calculates the shared session key $SK' = rand_1 \oplus rand_2$ and the authentication message $M_3 = SK' \oplus (rand_3 + 1)$. Then submits the authentication message M_3 to the substation SS_j. Otherwise, the appliance TR_i rejects the message and terminates the authentication process.

4) The substation SS_j upon receiving the message M_3 checks whether the value of the received M_3 equals to the value of the computed $SK \oplus (rand_3 + 1)$. If true, the substation SS_j sets SK as the shared session key with the appliance TR_i; otherwise, it terminates the authentication process.

5. Security Analysis of proposed protocol

C. BAN Logic

Perhaps the serious study about formal verification of cryptographic protocols began with logic of authentication by Burrows, Abadi, and Needham [20]. This article describes the rationale and verification of cryptographic protocols which known as BAN logic. A typical BAN logic sequence includes verification of message origin, message freshness, and the origin's trustworthiness. Like all axiomatic systems, BAN logic uses postulates and definitions to analyze authentication protocols.

BAN logic inspired much other similar formalism, such as GNY logic [22] which we will use it to evaluate our protocol. In some cases, a protocol was reasoned as secure by the BAN analysis but was in fact insecure. Of course, in certain cases, GNY logic also has some weaknesses when you use it to evaluate the desired protocol. For example, this logic does not recognize the reflection attacks, i.e. if smart appliance and substation have the same ID that leads to vulnerabilities against reflection attacks, GNY logic cannot detect them. We emphasize on the uniqueness of identifiers to avoid this vulnerability in the generating process of identities.

D. GNY Logic: Formulae and statements

In the GNY logic, a formula is a name used to refer to a bit string, which has a particular value in a run. To describe the GNY logic, first, let symbols X and Y range over formulae. Then, we will introduce some formulae used in our authentication proof [22].
1. (X, Y): the conjunction of two formulae X and Y.
2. $\{X\}_K$ and $\{X\}^{-1}{}_K$: symmetrically encrypt and decrypt X with the key K.
3. $\{X\}_{+K}$ and $\{X\}_{-K}$: asymmetrically encrypt and decrypt X with the public key +K and the private key -K.
4. $\oplus$: Exclusive-OR function.
5. $*X$: X is not originated here (i.e. it has not sent in current run).
Let symbols P and Q be principals. We will use the following statements in our proof.
1. $P \lhd X$: P is told formula X.
2. $P \ni X$: P possesses formula X.
3. $P | \sim X$: P once conveyed formula X.
4. $P | \equiv \#(X)$: P believes that X is fresh.
5. $P | \equiv \phi(X)$: P believes that X is recognizable.
6. $P | \equiv P \overset{S}{\leftrightarrow} Q$ believes that S is a suitable secret for P and Q.
7. $P | \Rightarrow X$: P has jurisdiction over X.
8. $P \lhd * X$: P is told that a formula X that did not convey previously in the current run.

E. Protocol descriptions and goals

We will change some notations to fit the GNY logic and our protocol. The private key and the public key of the server will denote as -K and +K, respectively.
1. $TR \rightarrow SS: (\{TRID_i \| \{TRID_i\}_S \| rand_1\}_{+K})$
2. $SS \rightarrow TR: (\{SSID_j \| rand_2\}_{rand1}, rand_3)$
3. $TR \rightarrow SS: (rand_1 \oplus rand_2) \oplus (rand_3 + 1)$
Now we describe our goals in detail.
(1) Message content authentication
Goal 1: SS believes the message in the first run is recognizable.

$$SS \mid \equiv \phi\{TRID_i \| \{TRID_i\}_S \| rand_1\}_{+K} \tag{1}$$

Goal 2: TR believes the message in the second run is recognizable.

$$TR \mid \equiv \phi(\{SSID_j \| rand_2\}_{rand1}, rand_3) \tag{2}$$

Goal 3: SS believes the message in the third run is recognizable.

$$SS \mid \equiv \phi((rand_1 \oplus rand_2) \oplus (rand_3 + 1)) \tag{3}$$

(2) Message origin authentication

Goal 4: TR believes SS conveyed the message in the second run.

$$TR \mid \equiv SS \mid \sim \{SSID_j \| rand_2\}_{rand1} \tag{4}$$

Goal 5: SS believes TR conveyed the message in the third run.

$$SS \mid \equiv TR \mid \sim ((rand_1 \oplus rand_2) \oplus (rand_3 + 1)) \tag{5}$$

(3) Session key material establishment

Goal 6: TR believes that SS believes that SK is a secret shared between TR and SS.

$$TR \mid\equiv SS \mid\equiv TR \xleftrightarrow{SK} SS \tag{6}$$

Goal 7: TR believes that SK is a secret shared between TR and SS.

$$TR \mid\equiv TR \xleftrightarrow{SK} SS \tag{7}$$

Goal 8: SS believes that TR possesses SK.

$$SS \mid\equiv TR \ni SK \tag{8}$$

Goal 9: SS believes that TR believes that SK is a secret shared between TR and SS.

$$SS \mid\equiv TR \mid\equiv TR \xleftrightarrow{SK} SS \tag{9}$$

F. Assumption list in proposed protocol

We will make some assumptions based on GNY logic as follows:

1. SS generates the secret key s, so it possesses s. SS also possesses the private key -K and the public key +K.

$$SS \ni s, SS \ni +K, SS \ni -K \tag{10}$$

2. Since SS keeps the identity table, SS believes that $TRID_i$ is recognizable.

$$SS \mid\equiv \phi(TRID_i) \tag{11}$$

3. Since TR stores $SEC_2 = SSID_jP$ secretly and holds the base point P. Then TR can check the $SSID_j$ and believes that $SSID_j$ is recognizable.

$$TR \mid\equiv \phi(SSID_j) \tag{12}$$

4. TR generates the random integer $rand_1$, so it possesses $rand_1$ and believes that $rand_1$ is fresh.

$$TR \ni rand_1, TR \mid\equiv \#(rand_1) \tag{13}$$

5. TR generates the random integer $rand_1$ as part of the session key in the current run. So, we assume that TR believes $rand_1$ is a suitable secret for himself and SS.

$$TR \mid\equiv TR \overset{rand_1}{\leftrightarrow} SS \tag{14}$$

6. SS generates the random integer $rand_2$ and $rand_3$, so it possesses $rand_2$ and $rand_3$, and believes that $rand_3$ is recognizable and $rand_2$ is fresh.

$$SS \ni rand_3, SS \mid\equiv \phi(rand_3), SS \ni rand_2, SS \mid\equiv \#(rand_2) \tag{15}$$

7. The SK generated by SS is a session key in the current run. So we assume that SS believes that SK is a suitable secret between itself and TR.

$$SS \mid\equiv SS \overset{SK}{\leftrightarrow} TR \tag{16}$$

8. TR believes that the server SS is an authority on generating a suitable session key material SK shared between TR and SS.

$$TR \mid\equiv SS \mid\Rightarrow TR \overset{SK}{\leftrightarrow} SS \tag{17}$$

G. Authentication proof using GNY logic [22]

(1) The first run:

$$\frac{SS \mid\equiv \phi(TRID_i), SS \ni s}{SS \mid\equiv \phi\{TRID_i\}_s,\ S \mid\equiv \phi(TRID_i \| \{TRID_i\}_s \| rand_1)} \quad 18)$$

If SS believes that $TRID_i$ is recognizable and SS possesses the key s, then SS is entitled to believe that the encryption of $TRID_i$ with the key s is recognizable and then the formula $\{TRID_i \| \{TRID_i\}_s \| rand_1\}$ is also recognizable.

$$\frac{SS \mid\equiv \phi(TRID_i \| \{TRID_i\}_s \| rand_1),\ SS \ni +K}{SS \mid\equiv \phi\{TRID_i \| \{TRID_i\}_s \| rand_1\}_{+K}} \tag{19}$$

If SS believes ($TRID_i\|\{TRID_i\}_s\|rand_1$) is recognizable and SS possesses a public key +K, then it believes that the encryption $\{TRID_i\|\{TRID_i\}_s\|rand_1\}_{+K}$ is recognizable. Therefore, in the proposed protocol, the server SS can recognize the message $\{TRID_i\|\{TRID_i\}_s\|rand_1\}_{+K}$ in the first run. (Goal 1)

(2) The second run:

$$\frac{TR\mid\equiv\phi(SSID_j),\ TR\ni rand_1}{TR\mid\equiv\phi(SSID_j\|rand_2), TR\mid\equiv\phi\{SSID_j\|rand_2\}_{rand1}} \tag{20}$$

If TR believes that $SSID_j$ is recognizable, then TR is entitled to believe that the formula ($SSID_j\|rand_2$) of which $SSID_j$ is a component, is recognizable. Since TR possesses $rand_1$, it also believes that the encryption $\{SSID_j\|rand_2\}_{rand1}$ is recognizable.

$$\frac{SS\mid\equiv\phi\{SSID_j\|rand_2\}_{rand1}}{SS\mid\equiv\phi(\{SSID_j\|rand_2\}_{rand1}, rand_3)} \tag{21}$$

If SS believes $\{SSID_j\|rand_2\}_{rand1}$ is recognizable, then it is entitled to believe that ◌̋($\{SSID_j\|rand_2\}_{rand1}$, $rand_3$) of which $\{SSID_j\|rand_2\}_{rand1}$ is a component, is recognizable. So, we can conclude that in the proposed protocol, TR can recognize the message ($\{SSID_j\|rand_2\}_{rand1}$, $rand_3$) in the second run, see (22) in Table 2. (Goal 2).

If the following five conditions hold:

1) TR receives the encrypted formula ($SSID_j\|rand_2$) with the key $rand_1$ and marked with a not-originated-here mark;
2) TR possesses $rand_1$;
3) TR believes that $rand_1$ is a suitable secret for himself and SS;
4) TR believes that the formula ($SSID_j\|rand_2$) is recognizable;
5) TR believes that $rand_1$ is fresh.

Then TR is entitled to believe that:

1) SS once conveyed ($SSID_j\|rand_2$) encrypted with $rand_1$
2) SS possesses $rand_1$. (Goal 4)

According to the GNY logic, we assume that $TR\mid\equiv SS\mid\Rightarrow SS\mid\equiv^*$, that is, TR believes that SS is honest and competent, and then we can deduce the (23) in Table.

If TR believes that SS is honest and competent; and TR receives a message ($\{SSID_j\|rand_2\}_{rand1}$, $rand_3$)$\sim>SS\mid\equiv TR\overset{SK}{\longleftrightarrow}SS$) which it believes SS conveyed, then TR ought to believe that SS believes TR $\overset{SK}{\longleftrightarrow}$ SS. Therefore, TR believes that SS believes that SK is a suitable secret between TR and SS. (Goal 6)

$$\frac{TR\mid\equiv SS\mid\Rightarrow TR\overset{SK}{\longleftrightarrow}SS,\ TR\mid\equiv SS\mid\equiv TR\overset{SK}{\longleftrightarrow}SS}{TR\mid\equiv TR\overset{SK}{\longleftrightarrow}SS} \tag{24}$$

If TR believes that SS is an authority on the statement TR $\overset{SK}{\longleftrightarrow}$ SS and SS believe in TR $\overset{SK}{\longleftrightarrow}$ SS, then TR ought to believe in TR $\overset{SK}{\longleftrightarrow}$ SS as well. So, TR believes that SK is a suitable secret between TR and SS. (Goal 7)

(3) The third flow:

$$\frac{SS\triangleleft\{TRID_i\|\{TRID_i\}_s\|rand_1\}_{+K},\ SS\ni -K}{SS\triangleleft(TRID_i\|\{TRID_i\}_s\|rand_1),\ SS\triangleleft rand_1} \tag{25}$$

If SS is told a formula ($TRID_i\|\{TRID_i\}_s\|rand_1$) encrypted with the public key +K and it possesses the corresponding private key -K, then that is considered to have been told the plain contents of that formula, and it has also been told $rand_1$ a

$$\frac{SS\triangleleft rand_1,\ SS\ni rand_2,\ SS\ni rand_3}{SS\ni rand_1,\ SS\ni(rand_1\oplus rand_2),\ SS\ni(rand_3+1)} \tag{26}$$

If SS is told $rand_1$, it is capable of possessing $rand_1$, and if SS also possesses $rand_2$, it is capable of possessing ($rand_1\oplus rand_2$). For the same reason, if SS possesses $rand_3$ then it possesses ($rand_3$ +1).

$$\frac{SS\ni(rand_1\oplus rand_2),\ S\ni(r_3+1)}{SS\ni((rand_1\oplus rand_2)\oplus(rand_3+1))} \tag{27}$$

If SS possesses ($rand_1\oplus rand_2$) and ($rand_3$ +1), then it possesses ($rand_1\oplus rand_2$) ⊕ ($rand_3$ + 1) as well.

$$\frac{SS\mid\equiv\phi(rand_3)}{SS\mid\equiv\phi((rand_1\oplus rand_2)\oplus(r_3+1))} \tag{28}$$

If SS believes that $rand_3$ is recognizable, then SS believes that ($rand_3$ +1) is recognizable and (($rand_1\oplus rand_2$)⊕($rand_3$ + 1)), of which ($rand_3$ +1) is a component, is also recognizable, see (29) in Table 2.

If SS believes that ($rand_1\oplus rand_2$)⊕($rand_3$ + 1) is recognizable and it also possesses ($rand_1\oplus rand_2$)⊕($rand_3$ + 1), then it is entitled to believe that ($rand_1\oplus rand_2$)⊕($rand_3$ + 1) is recognizable. So, we can say that SS believes that the message ($rand_1\oplus rand_2$)⊕($rand_3$ + 1) in the third run is recognizable. (Goal 3)

$$\frac{SS\mid\equiv \#(rand_2),\ SS\ni(rand_1\oplus rand_2)}{SS\mid\equiv \#(rand_1\oplus rand_2)} \tag{30}$$

If SS believes $rand_2$ is fresh, then it is entitled to believe that ($rand_1\oplus rand_2$) is fresh. If SS also possesses ($rand_1\oplus rand_2$),

it is entitled to believe that ($rand_1 \oplus rand_2$) is fresh, see (31) in Table 2.
If all of the following conditions hold:
1) SS receives a formula consisting of a XOR function of ($rand_3$+1), and SK marked with a not-originated-here mark;
2) SS possesses ($rand_3$+1) and SK;
3) SS believes SK is a suitable secret for itself and TR;
4) SS believes that SK is fresh. Then SS is entitled to believe that TR once conveyed (($rand_3$+1), SK) and (($rand_1 \oplus rand_2$)$\oplus$($rand_3$+1)).Therefore, we can say that SS believes that the message (($rand_1 \oplus rand_2$)$\oplus$($rand_3$+1)) has conveyed from the TR in the third run of our protocol. (Goal 5)

$$\frac{SS|\equiv TR|\sim((rand_3+1),SK),\ SS|\equiv \#(SK)}{SS|\equiv TR|\sim SK,\ SS|\equiv TR \ni SK} \qquad (32)$$

If SS believes that TR once conveyed the formula (($rand_3$+1), SK), then it is entitled to believe that TR once conveyed SK. And if SS also believes that SK is fresh, then it is entitled to believe that TR possesses SK. Therefore, SS believes that TR possesses SK. (Goal 8)

Now, we assume that SS $|\equiv$ TR $|\Rightarrow$ TR $|\equiv^*$, that is, SS believes that TR is honest and competent, and then we can deduce (33) in Table 2.
If SS believes that TR is honest and competent, and SS receives a message (SK$\oplus$($rand_3$+1))~>TR|≡TR$\overset{SK}{\leftrightarrow}$SS which it believes is conveyed by TR, then SS ought to believe that TR believes TR$\overset{SK}{\leftarrow\rightarrow}$SS. Thus, we can conclude that in our protocol, SS believes that SK is a suitable secret between TR and SS. (Goal 9)

6. Complexity Analysis of the protocol

Now, we want to describe the functionalities of our proposed protocol and evaluate the computational cost of it. We compare the computational cost of our protocol with the protocols proposed by [3], [4] and [5].
First, some notations are defined as follows:

1. T_m: the time for executing a modular exponentiation operation.
2. T_e: the time for executing a scalar multiplication operation of an elliptic curve.
3. T_h: the time for executing a one-way hash function.
4. T_{se}: the time for executing a secret key encryption operation.
5. T_{sd}: the time for executing a secret key decryption operation.
6. T_{ae}: the time for executing a public key encryption operation.
7. T_{ad}: the time for executing a public key decryption operation.
8. T_{hmac}: the time for executing an HMAC[1] operation.
9. T_x: the time for executing an exclusive-or function.

As shown in Table 1, during the initialization phase of our proposed protocol, the computational cost at the substation SS_j side is T_e+T_{se}. One secret key encryption operation T_{se} is used to generating secret $SEC_1 = E_s(TRID_i)$ through using the system key s, and one scalar multiplication operation T_e is used to compute the another secret $SEC_2 = SSID_jP$. The computational cost at the substation SS_j side is T_{ad} +T_x +T_{sd}+ T_{se}, and the computational cost at the appliance TR_i side is T_{ae} +T_{sd} + T_e + T_x in the authentication phase. The appliance TR_i takes one public key encryption operation via the substation SS_j's public key k_{pu} to generate $M_1 = e_{kpu}(TRID_i \oplus SEC_1 \oplus rand_1)$; takes one secret key decryption operation to get $SSID_j$ and $rand_2$; takes one scalar multiplication operation to compute $SSID_jP$, and takes an XOR function operation to calculate M_3 = (SK'$\oplus$($rand_3$ + 1)).

The substation SS_j takes one public key decryption operation to get the appliance TR_i's identity $TRID_i$, the random integer $rand_1$ and the authentication message SEC_1; takes an XOR function operation to obtain (SK$\oplus$($rand_3$+1)), and takes one secret key decryption operation and one secret key encryption operation.

Table 1- Computational costs comparison between the proposed protocol and three others.

	Our protocol	Chim et al.'s protocol [3]	Mostafa et al.'s protocol [4]	Zhang et al.'s protocol [5]
Smart appliance	T_{ae} +T_{sd} + T_e + T_x	$2T_{ae}$+T_{hmac}	_____	T_{ae} +T_{sd} + T_e + T_h

[1] Hash-based Message Authentication Code

Substation	$T_e + T_{ad} + T_x + T_{sd} + 2T_{se}$	T_{hmac}	_____	$T_e + T_{ad} + T_h + T_{sd} + 2T_{se}$
Control center	_____	$2T_{ad}$	_____	_____
HAN	_____	_____	$2T_m+T_{ae}+T_{ad}+T_h+T_{hmac}$	_____
BAN	_____	_____	$2T_m+T_{ae}+T_{ad}+T_h$	_____
Total	$2T_e+T_{ae}+T_{ad}+2T_{sd}+2T_{se}+2T_x$	$2T_{ae}+2T_{ad}+2T_{hmac}$	$2T_{ae}+2T_{ad}+2T_h+4T_m+T_{hmac}$	$2T_e+T_{ae}+T_{ad}+2T_{sd}+2T_{se}+2T_h$
Storage overhead	2240 bits	3232 bits	_____	3200 bits

Table 2- Statements

$$\frac{TR\lhd^{*}\{SSID_j\|rand_2\}_{rand1},\ TR\ni rand_1, TR|\equiv TR\overset{rand_1}{\leftrightarrow}SS,\ TR|\equiv\phi(SSID_j\|rand_2),\ TR|\equiv \#(rand_1)}{TR|\equiv SS|\sim\{SSID_j\|rand_2\}_{rand1},\ TR|\equiv SS\ni rand_1} \tag{22}$$

$$\frac{TR|\equiv SS|\Rightarrow SS|\equiv^{*},\ TR|\equiv SS|\sim(\{SSID_j\|rand_2\}_{rand1},rand_3)\sim>SS|\equiv TR\overset{SK}{\leftrightarrow}SS),\ TR|\equiv\#(\{SSID_j\|rand_2\}_{rand1},rand_3)}{TR|\equiv SS|||\equiv TR\overset{SK}{\leftrightarrow}SS} \tag{23}$$

$$\frac{SS|\equiv\phi((rand_1\oplus rand_2)\oplus(rand_3+1)),\ SS\ni((rand_1\oplus rand_2)\oplus(rand_3+1))}{SS|\equiv\phi((rand_1\oplus rand_2)\oplus(rand_3+1))} \tag{29}$$

$$\frac{SS\lhd^{*}\ ((rand_3+1)\oplus<SK>),\ SS\ni((rand_3+1),SK),\ SS|\equiv SS\overset{SK}{\leftrightarrow}TR,\ SS|\equiv\#(SK)}{SS|\equiv TR|\sim((rand_3+1),<SK>),\ SS|\equiv TR|\sim((rand_3+1)\oplus<SK>)} \tag{31}$$

$$\frac{SS|\equiv TR|\Rightarrow TR|\equiv^{*},\ SS|\equiv TR|\sim((SK\oplus(rand_3+1))\sim>TR|\equiv TR\overset{Sl}{\leftrightarrow}SS),\ SS|\equiv\#(SK\oplus(rand_3+1))}{SS|\equiv TR|\equiv TR\overset{Sl}{\leftrightarrow}SS} \tag{33}$$

Thus, the total computational cost of our protocol is $T_{ae}+T_{ad}+2T_e+2T_{se}+2T_{sd}+2T_x$. The public key cryptographic operations T_{ae}/T_{ad} and the modular exponentiation operation T_m are much higher than that of the scalar multiplication operation of elliptic curve T_e and the secret key cryptographic operations T_{se}/T_{sd}. Also, compared with the modular exponentiation operation T_m and the public key cryptographic operations T_{ae}/T_{ad}, the computational cost of XOR function operation T_x is very low and could be ignored. Close analysis of the data in Table 1, shows that our proposed protocol is more efficient than Mostafa et al.'s protocol [4] because it reduces the numbers of public key cryptographic operations and eliminates the expensive modular exponentiation operations. Also, compared with Chim et al.'s protocol [3], the proposed protocol reduces the computational cost at the appliance side. In comparison with our protocol, Chim et al.'s protocol possess better performance at the substation side, but their protocol fails to provide a key agreement and cannot support mutual authentication. In comparison with Zhang et al.'s protocol [5], our proposed protocol has better performance to storage overhead in tamper-resistance device side.

Now, we compare storage overhead of our protocol with three other protocols. Since Mostafa's protocol [4] don't use the tamper-resistant device, we compared storage overhead with Zhang et al.'s protocol [5] and Chim et al.'s protocol [3] at the appliance side. In the proposed protocol, the appliance needs to store the secure information (SEC, k_{pu}, P) and an identifier $TRID_i$, where SEC is 1056 bits, P is 1024 bits, K_{pu} is 128 bits, and $TRID_i$ is 32 bits. In our protocol, the total storage overhead needed at the smart cards is 2240 bits. In Chim's protocol [3], the tamper-resistant needs to store the secret key S_r, the public key Pub_{cc}, a pair private and public key, HMAC function and the identity of appliance RID_i. Where S_r is 128 bits, Pub_{cc} is 1024 bits, the pair key is 2048 bits, and RID_i is 32 bits. Thus, the total overhead at the tamper-resistant devices side in Chim's protocol [3] is 3232 bits.

In Zhang et al.'s protocol, the tamper-resistant device needs to store the secure information (C_1, C_2, p_K, P), and a hash function, where C_1, C_2, and P are 1024 bits, and p_k is 128 bits. So the total storage overhead needed at the tamper-resistant devices is 3200 bits. As shown in Table 1, Compared with other protocol, our proposed protocol reduced the storage overhead at the tamper-resistant side.

7. Recommendations

It is evident that to establish comprehensive security in a wide network such as smart grid; we should consider all security aspects and different threats. So, in addition to physical security that is an important issue to protect the control center and substations, using the equipment with Tempest standard to minimize electromagnetic radiation of control center and substations that cover vital regions is critical. Although the equipment with this standard has a high price, security has the cost of its own. Also to prevent attacks such as electromagnetic bombs or graphite bombs which are a non-lethal weapon used to disable electrical power systems, the solutions should consider by the relevant authorities for crisis situations. Graphite bombs spread a cloud of extremely fine carbon filaments over electrical components and cause to disrupt the electrical supply. So, the passive defense as a set of unarmed measures will reduce such vulnerability. On the one hand, passive measures increase defense capability in times of crisis and on the other hand reduce the consequences of the crisis and provide the possibility of damaged areas recovery with the lowest cost. Thus, we should pay attention to these safety measures in smart grids.

8. Conclusion

In this paper, an efficient authentication protocol based on elliptic curve cryptography with identity protection for smart grids has been proposed which can deploy in UTM systems. In the proposed protocol, the substations and smart appliances realized mutual authentication and key agreement via a tamper-resistant smart card. The identities of the substation and the appliance are encrypted and transmitted in our protocol. So the adversary cannot access to the real identities of the substation and the appliance. Furthermore, the adversary cannot establish an impersonation attack to inject false data into the system. Thus, it can prevent the LR attacks in smart appliance side. We demonstrated the completeness of the proposed protocol by Gong, Needham, and Yahalom logic. In comparison with other related protocols, performance analysis shows that our protocol increases efficiency. Thus, we believe that our protocol is more suitable for the smart grids.

References

[1] ARC Advisory Group, SCADA Systems for Smart Grid, Available: http://www.arcweb.com/Research/Studies/Pages/SCADA-Power.aspx.

[2] Salem AA. Electricity agents in smart grid markets. Computers Industry. 2013; 64(3):235–241.Compind.2012.10.009. doi: 10.1016/j.

[3] Chim TW, Yiu SM, Hui LCK, Li VOK. PASS: Privacy-preserving Authentication Scheme for Smart Grids Network. Proceedings of Cyber & Physical Security & Privacy. 2011; 196–201. 6102316

[4] Mostafa M, Fadlulah ZM, Kato N, Lu , Shen . A Light-weight Message Authentication Scheme for Smart Grids Communications. IEEE Transaction on Smart Grid. 2011; 2(4): 675–685.

[5] Liping Zhang, Shanyu Tang, He Luo, Elliptic Curve Cryptography-Based Authentication with Identity Protection for Smart Grids, PLOS 2016, http://journals.plos.org/plosone.

[6] Li QH, Cao GH. Multicast Authentication in the Smart Grid with One-Time Signature. IEEE Transaction on Smart Grid. 2012; 2(4) 686–696.

[7] Oh S, Kwak J. Mutual Authentication & Key Establishment mechanism using DCU certificate in Smart Grid. Applied Mathematics & Information Sciences. 2012; 6(1S): 257S–264S.

[8] Nam J, Choo KKR, Han S, Kim M, Paik J, Won D. Efficient & Anonymous Two-Factor User Authentication in Wireless Sensor Network: Achieving User Anonymity with Lightweight Sensors Computation. Plos one, 2015; 10(4): 1–21.

[9] He D, Kumar N, Chilamkurti N. A secure temporal-credential-based mutual authentication & key agreement scheme with identity for wireless sensor networks. Information Sciences. 2015; 321: 263–277.

[10] Gao QH. Biometric Authentication in Smart Grid. Proceedings of Energy & Sustainability Conference. 2012; pp.1–5.

[11] He D, Zeadally S. Authentication protocol for ambient assisted living system. IEEE Communications Magazine, 2015; 53(1):71–77.

[12] Wang CQ, Zhang X, Zheng ZM. Cryptanalysis & Improvement of a Biometric-Based Multi-Server Authentication & Key Agreement Scheme. Plos one, 2016; 11(12):1–25.

[13] Vaidya B, Markakis D, Mouftah HT. Authentication & Authorization Mechanisms for Substation Automation in Smart Grid Networks. IEEE Network. 2013; 5–11.

[14] Liu H, Ning HS, Zhang Y, Guizani M. Battery Status-aware Authentication Scheme for V2G Networks in Smart Grid. IEEE Transactions on Smart Grids. 2013; (4) (1):99–110.

[15] Nicanfar H, Leung VCM. Password authenticated cluster based group key agreement for smart grid communication. Security & Communication Network. 2014; 7(1): 221–233.

[16] Zhang L, Tang S, Jiang Y, Ma Z. Robust & Efficient Authentication Protocol Based on ECC for Smart Grids. 2013 IEEE International Conference on Green Computing

& Communications & IEEE Internet of Things & IEEE Cyber, Physical & Social Computing, 201; 2089–2093.

[17] Nicanfar H, Leung VCM. Multilayer Consensus ECC-Based Password Authenticated Key-Exchange Protocol for Smart Grid System. IEEE Transaction on Smart Grid. 2013; 4(1): 253–264.

[18] He D, Kumar N, Lee JH. An efficient & privacy preserving data aggregation scheme for the smart grids against internal attackers. Wireless Network. 2016; 22(2): 491–502.

[19] Li D, Aung Z, Williams JR, Sanchez A. Efficient & fault-diagnosable authentication architecture for AMI in the smart grid. Security & Communication Networks. 2015; 8(4):598–616.

[20] Burrows M, Abadi M, Needham R. Logic of authentication. ACM Transaction on Computer Systems. 1990; (8): 18–36.

[21] Nessett DM. A critique of the Burrows, Abadi, & Needham logic. ACM SIGOPS Operating Systems Review. 1990; 24(2):35–38.

[22] Li Gong, Needham R, Yahalom R. Reasoning about belief in cryptographic protocol. Proceedings of IEEE Computer Society Symp. Research in Security & Privacy. 1990; 234–248.

[23] Fan CI, Lin YH. Provably Secure Remote Authentication Scheme with Privacy Protection on Biometrics. IEEE Transactions on Information Forensics & Security. 2009; 4(4):933–945.

[24] Darrel H, Alfred M, Scott Vanstone. Guide to elliptic curve cryptography. 2004; Springer-Verlag, Berlin.

[25] Kilinc HH, Yanik T. A Survey of SIP Authentication & Key Agreement Schemes. IEEE Communications Surveys& Tutorials. 2013; 1–19.

[26] Adnan A, Abdul N.M, Zahir T, Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid, Elsevier-Science Direct, Information Systems, Volume 53, October–November 2015, Pages 201–212.