SECURE KEY MANAGEMENT SCHEME FOR AMI IN SMART GRID

Mohammad Hossein Yaghmaee

Mashhad Electric Energy Distribution Company (MEEDC), Iran
yaghmaee@ieee.org

Azadeh Javid Hassani

Mashhad Electric Energy Distribution Company (MEEDC), Iran
azadehjavid@gmail.com

ABSTRACT

The smart grid has been introduced as the next generation power grid. Advanced Metering Infrastructure (AMI) is one of the key components in this grid. It provides bidirectional communication between consumers and management entities in the utility side. This bidirectional nature communication flow has made AMI vulnerable to various cyber attacks. So, cyber security has become an important concern in this context. Key management for securing communications between a large amount of smart meters (SMs) and a master station (MS) in the utility premise is one of the most important components of the AMI security protocols. AMI has special characteristics and features in comparison with other IT systems, to design an efficient scheme these features should be considered. Features like resource constraints of smart meters and low bandwidth of communication lines. In this paper we are going to design a light weight key management scheme with a novel key refreshment policy that decrease the network overhead, which makes symmetric keys to secure communications between SMs and MS using elliptic curve cryptography (ECC) parameters and simple cryptographic algorithms like hash functions.

Index terms: AMI, smart meter, master station, key management, ECC

INTRODUCTION

AMI acts as an interface with the capability for managing the communications between smart meters and devices in home premise and management systems in the utility premise in a bidirectional manner. This technology replaces the old one-way Advanced Meter Reading (AMR) technology. It enables utilities or service providers to give their customers real time electricity pricing information [1]. Therefor, cyber security of the AMI system becomes crucial and should be considered prior to its applications [2]. Hybrid transmission modes of messages in AMI has made this system more vulnerable to cyber attacks [2]. In general AMI has four fundamental security requirements: confidentiality, integrity, availability and non-repudiation. Privacy of the customer's sensitive data like metering and energy consumption is the most important issue of confidentiality in AMI. Customers don't want any unauthorized person or even marketing companies to gain information about their amount of energy usage or energy usage pattern. Integrity in AMI is not just important for the sensitive data that is stored in smart meters or transmitted over the communication channels but also integrity of control commands is very crucial. It means that transmission of unauthorized commands through the AMI system to customer premise should be prevented. Consider an adversary can masquerade as a master station and sends disconnect commands to a large mound of smart meters and makes a big disaster for the utility and consumers [5]. So message authentication is important to be supported in the AMI. In comparison with the AMR systems, the AMI with much more than meter readings being exchanged between smart meters and utility premise, availability of information and control commands in the AMI system has become important [5]. Denial of service attack (DOS) can threaten availability. As mentioned before to resolve confidentiality and integrity encryption and authentication methods is utilized and security of them depends on the security of cryptographic keys [2]. Key management has gained attention of researchers and although there have been several studies on this subject lately, but it is not a decently solved problem up to now.

In [2], the authors propose a solution for key management between a management entity like MDMS in the utility and devices in home premise (i.e., smart meters and user gateways). Their approach has three different schemes for unicast, broadcast, and multicast communications. The proposed solution for multicast in needs key freshness and redistribution each time a member joins or leaves the group and with a group of n members, at last $2\,\mathrm{Log}_2\, n$ key encryptions and message transmissions is needed. This scheme hasn't taken considerations into network topology. We are going to use some of their design ideas in our model.

In [3] the authors propose a key agreement between utility and smart meters. In their solution they use a CA as a security associate in the utility side. The authors propose an ID-based model with a one way hash function to provide the public each of each node based on its ID. Whenever a new mart meter wants to join the network, SM and SA are mutually authenticated through a synchronization phase that is done with the help of a previously initialized node called AG. This phase includes several symmetric and asymmetric encryption operations between involved entities that increases the computational overhead of this scheme. This phase could be done offline to decrease this overhead.

In [6] authors propose a group ID-based solution to establish the keys for large amount of entities (home appliances). In this scheme all the entities use the same

key (group key) for their communications with user gateway and this could decrease the security of information every appliance.
The authors of [9] explain the importance of key management in AMI systems.
Most of the key management solutions proposed for the AMI utilize ID-based or PKI-based mechanisms. We know that directly implementation of none of these mechanisms is suitable for AMI mechanisms. PKI has the problem of maintaining the certificates that have a high cost and also making them void. ID-based mechanisms have the problem of key escrow. Besides in both of these mechanisms at the time of power outage the CA or PKG won't be available and can't do their duty in the process of key management. Due to these problems, in this work we have designed a key management scheme that uses ECC parameters to agree symmetric keys between the MS and a large amount of SMs. Because we don't use ECC for public cryptography mechanisms we won't need to use CA or certificates. We also propose a novel key refreshing policy that decreased the network overhead at the time of new key distribution. Our scheme also supports end to end authentication.
The rest of our paper is organized as follows. Sections I and II include technical required background about AMI and ECC. In section III our key management scheme will be proposed. We will analyze the performance and security of our scheme respectively in section IV and V. Section VI is the conclusion of the current work.

I. AMI ARCHITECTURE AND ITS SECURITY CHALLENGES

As mentioned before the AMI is a system that collects, measures and analyzes the energy consumption of customers. In this section we are going to explain those components of this system that is involved in the key management process and also challenges and special features of the AMI that affects designing a security protocol.

AMI system components

Smart meter: They are solid-state and programmable and do a lot of functions like metering and measuring in a bidirectional manner, realtime time-based pricing, remote turn on or turn off operations, etc.
Communication networks: There is a hierarchy of communication networks in the AMI and they can be generally classified as follows

- Wide area network (WAN): it is a network between the utility and the concentrator. The concentrator aggregates the data from meters and sends them to MDMS.
- Neighbor area network (NAN): it connects smart meters to the concentrator.
- Home area network (HAN): it is a local area network and is usually composed of home appliances that communicate with each other and the smart meter. It also acts as a path that utilities utilize to reach the devices inside the home.Smart grid is presumed to have an IPV6 topology for it's communication networks outside of the HAN. A mesh based topology with a high probability of utilizing the WiMax communication. For inside the HAN, usually the ZigBee and 6LoWPAN are the attainable technology. In point of fact, IEEE 802.16 is the standard for outside and IEEE 802.15.4 is the standard for inside the HAN domain [3].

Meter data management system (MDMS): It is a database that stores meter data with analytical tools and is in contact with AMI headend. It also interacts with other systems of he utilities through enterprise bus.

Security challenges and constraints in the AMI

As mentioned before the storage and computational ability of SMs are limited and there are bandwidth limitations in the communication networks of AMI. Also, because there is realtime transmission of information in the AMI, the computation time of cryptographic operation for generating the session keys should be as minimum as possible.

II. ELLIPTIC CURVE CRYPTOGRAPHY

Because of the dozens benefits of ECC, it has been utilized in various environments, particularly in systems with resource constraint entities and. One of the most important benefits of ECC is providing the same level of security with smaller key size in comparison with other cryptographic techniques like RSA. For example, ECC with 160 bit keys provide the same level of security as RSA, D-H cryptography with 1024 and 15360 bit keys, respectively. In addition to addressing the resource constraint issue, ECC is also beneficial in enabling an efficient protocol that supports current and future devices with various levels of technology, which is important in emerging AMI technology.
Generally ECC is presented as an Elliptic curve with points (x, y) over Z_p with the following definition [4]:

$$\begin{cases} y^2 \equiv x^3 + a + b mod p \\ where: (x,y) \in Z_p \\ s.t \;\; p > 3 \; (a \; large \; prime), a, b \in Z_p \end{cases}$$

III. ECC-BASED KEY MANAGEMENT SCHEME

In this section we are going to propose our ECC-based key management scheme for unicast and broadcast communications. Our scheme is composed of key generation and refreshment.

Basic definitions and parameters

1) m: number of SMs
2) a and b: two field elements that define the ECC equation
3) p: field size
4) G: base point. An ECC that generates the subgroup of order n
5) n: order of point G
6) d_i: private value of each entity from interval $[1, n-1]$, i=0,…, m
7) Q_0: public value for key generation
8) R_i: a random number for key generation
9) H (K): a one way hash function
10) $HMAC_k$ (M): a keyed massage authentication function that uses k as key
11) X|Y: concatenation of X and Y
12) Random (b): a function that generates a b-bit random number
13) SK_i: a symmetric key for message encryption. i=0 for broadcast mode
14) E_{SK} (data): a symmetric encryption function that uses SK as cryptographic key
15) DE_{SK} (Edata): a symmetric decryption function that uses SK as cryptographic key
16) V_s and V_r: verifiers at the sending and receiving end respectively

System initialization for key management

In this phase MS generates required values and distributes them to smart meters through a secure channels (e.g. like using a smart card for every SM). Step1:MS can use special key servers for it's initial value generation. MS first chooses d_i, i=0,…, m from the interval $[1, n-1]$, and generates R_i=Random (b) and computes $Q_0=d_0G$ that we will call it the public value because it is built like the public key on ECC based public cryptography, but won't be used for asymmetric cryptography operation, we are going to use it in our session key generation scheme. Then stores d_i and R_i of each SM and d_0 and R_0 in its private domain. Q_0 doesn't need to be private because based on Elliptic Curve Discrete Logarithm Problem (ECDLP) if an attacker has G and Q0 it is very hard to find d0.
Step2: before deployment every SM securely accesses the key server in MS to be loaded with {d0, Q0,R0} and its {Ri, di} and required ECC parameters. di and d0 will be stored in a tamper resistant memory in the SM.

Key generation and message verification for Unicast communications

Unicast messages in the AMI can be transmitted from MS to SM and reverse. To provide the confidentiality and integrity of messages session key should be refreshed at every session. Fig. 1. Shows the scheme in details
Step1: sender generates the session key and uses it (SM or MS)

$$Q_i = d_i Q_0$$
$$SK_i = H(H(Q_i)|H(R_i))$$
$$EData = E_{sk_i}(Data)$$
$$V_s = HMAC_{sk_i}(EData)$$

Step2: message transmission. The end system forms following packet, and sends it through communication channels:
$MS(SM) \rightarrow MS(SM): (Edata, V_s)$
Step3: message verification and decryption at receiving side:

$$Q_i = d_i Q_0$$
$$SK_i = H(H(Q_i)|H(R_i))$$
$$V_r = HMAC_{sk_i}(EData)$$

If $V_r = V_s$

$$Data = DE_{SK_i}(Data)$$

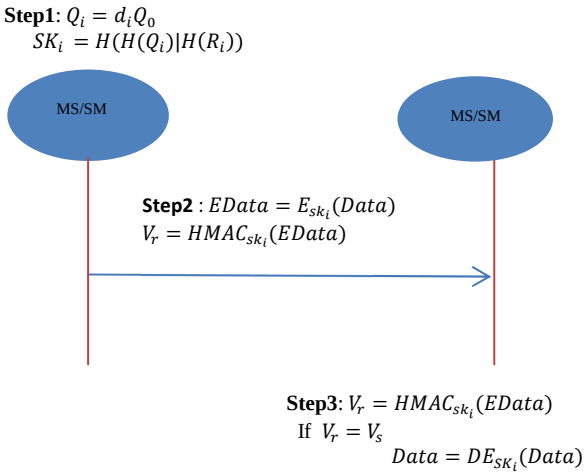

Fig. 1. Key generation and message verification for Unicast communications

Key generation and message verification for broadcast communications

Broadcast messages can just be transmitted from MS SMs. Like unicast messages to ensure confidentiality and integrity session keys should be refreshed before every broadcast session. Fig. 2. Shows the scheme in details
Step1: sender generates the session key and uses it (MS to SMs)

$$Q_{ms} = d_0 Q_0$$
$$SK_{ms} = H(H(Q_{ms})|H(R_{ms}))$$
$$EData = E_{sk_{ms}}(Data)$$
$$V_s = HMAC_{sk_{ms}}(EData)$$

Step2: message transmission. MS forms the below packet, and broadcast it to all SMs
$MS \rightarrow SM_i (i = 1, 2, \dots, m): (Edata, V_s)$
Step3: message verification and decryption at receiving side (SMs)

$$Q_{ms} = d_0 Q_0$$

$$SK_{ms} = H(H(Q_{ms})|H(R_{ms}))$$
$$V_r = HMAC_{sk}(EData)$$

If $V_r = V_s$

$$Data = DE_{SK}(Data)$$

Key refreshment policy

To maintain key freshness and security of the scheme, private values (d_i, $i = 0\ to\ n$) should be refreshed periodically. Because we use ECC parameters in our scheme that brings more security with the same size of the key in comparison with other methods and due to the ECDLP finding d_i with having Q_i and Q_0 is

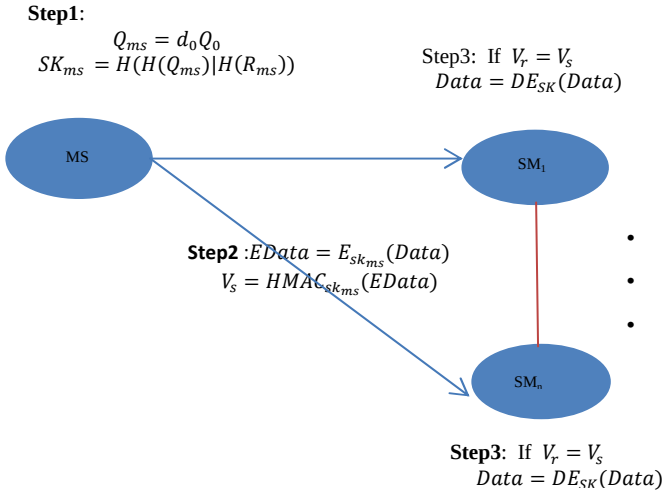

Fig. 2. Key generation and message verification for broadcast communications

Computationally very hard the period that the keys need to be refreshed in, will increase in comparison with other solutions like the one in [2]. To achieve this goal a hash function H_2 will be applied to d_i ($i = 0\ to\ n$) . To decrease the overhead of the network at the time of key refreshment, in our scheme SMs will able to generate the new d_i themselves. H_2 will be loaded in the SM by technicians at the time of installing it, therefor every SM can refresh its own d_i. MS also will send a broadcast message to SMs that includes the Update Time (UT). The UT is the time that SMs should renew their d_i and d_0. MS also will renew each SM's d_i and d_o at UT. MS and SMs should be synchronized, which the design is outside of the scope of this paper.

IV. PERFORMANCE ANALYSIS

For analysis of our scheme, we present operation time of cryptographic operations that we have utilized: TG_{mul}:the time of executing a point scalar multiplication, TG_h:the time of executing a one way hash function, TG_{con}: the time of executing a concatenation tat is too small to be taken in consideration. They have been listed table I. The operations were built with a standard cryptography library named MIRACLE and the hardware platform is a 32bit operating system and an Intel A80386-16MHz processor with 256-MB memory for a SM and INTEL Pentium 4.3.2 GHz with 1G memory for MS.

Table I. cryptographic operation time (in milliseconds)

	TG_{mul}	TG_h	TG_{con}
MS	0.83	<0.0001	very low
SM	12.08	<0.001	very low

A. Storage cost

For implementation of our scheme, related data Including private values and random numbers should be stored on the SMs and MS. In actual implementations, for a symmetric cryptographic algorithm (e.g. AES) usually a 128 or 256 bit long key is used. We will use 128-bit-long key with the same length of a random number. Q_0 will be stored in 128 bit binary manner.
MS can use key management servers as storage for the key management related data. Therefor storage cost won't be a problem. In contrast SMs have limited storage space. Therefor, we should try to decrease the key management related data that should be stored in SMs. According to the table II the data that should be stored on each SM won't exceed $(5 \times 128)/8 = 80$ bytes that it is acceptable for the aforementioned SM.

Table II. Related data stored in MS and SMs

	MS	**SMs(SM_1 to SM_n)**
Public value	Q_0	Q_0
Unicast	$d_1, \ldots, d_m$ $R_1, \ldots, R_m$	d_i, R_i
Broadcast	d_0, R_0	d_0, R_0

B. Time consumption cost:

As transmission of messages is time limited, we analyze the time cost of the cryptographic operations for key generation at the MS and SMs. The key generation cryptographic operations that are the same for unicast and broadcast mode, are listed in table III. According to table I and table III, the time consumption of session key generation in the MS and SMs has been computed and proposed in table IV. From the results in table IV the key generation delay is acceptable.

Table III. key generation cryptographic operations

	Hash	point multiplication
MS	$3T_h$	$1T_{mul}$
SM	$3T_h$	$1T_{mul}$

Table IV. key generation time consumption

MS	0.8303 ms
SM	12.083 ms

V. SECURITY ANALYSIS

In order to prove the security of our scheme, we introduce some attacks and then show that our scheme is secure against them.

1. Denial Of Service (DOS): because our scheme doesn't have any request phase in the key generation process and MS itself distribute the related data securely, so adversary can't perform a DOS with sending a request message repeatedly.
2. Man In The Middle (MITM) attack: because related data are distributed securely to SMs and after that before every session SK is generated on every side with any message transmission in the key generation phase, therefore, there is no packet that an adversary can capture to perform a MITM attack.
3. Replay attack: because session key SK updates before every session with updating R_i, the attacker can't perform a Replay attack on the messages that is being transmitted. If he or she eavesdrop one of the messages it is not possible to use it again.
4. Insider attack: a malicious insider would want to perform DOS or MITM attack. Because of the reasons mentioned above for these two attacks, an insider won't be able to perform any of these attacks.
5. Denning-sacco attack : assume that an adversary can find the SK of one of the sessions. Because of using concatenation operator and hash functions he or she will find them, due to the ECDLP won't be able to find d_i,d_0 that are the secret keys.
6. Impersonation attacks : by using the HMAC function our solution supports mutual authentication between the MS and SMs, therefor, an impersonation attack can't be performed by an adversary.

VI. CONCLUSION

In this study, we presented a key management scheme for unicast and broadcast communications in the AMI. We proposed a novel key refreshing policy that decreases the network overhead since we know we have the bandwidth constraint of communication networks and need to provide real time message delivery. By using the ECC parameters in our session key generation mechanism, we bring higher security with the same size of the key to our approach. The storage space and time consumption of our scheme is suitable for the AMI due to the resource constraint of SMs, it also supports end to end mutual authentication.

REFRENCES

[1] M. Badra, SH.Zeadally, 2013, " key management solutions in the smart grid environment ", ieeeexplore.ieee.org
[2] N. Liu, J. Chen, L. Zhu, J. Zhang, Y. He, 2012, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid", IEEE Transactions on Industrial Electronics, vol. 60, 4746-4757
[3] H. Nicanfar, P. Joker, V. C. M. Leung, 2011, "Smart Grid Authentication and Key Management for Unicast and Multicast Communications", IEEE PES Innovative Smart Grid Technologies, 1 – 8
[4] H. Nicanfar, V. C. M. Leung, 2013, "Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System", IEEE Trans. Smart Grid, Vol. 4, 253-264
[5] F. M. Cleveland, 2008, "Cyber security issues for advanced metering infrastructure (AMI)" IEEE Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, 1–5
[6] J. Kamto, L. Qian, J. Fuller, J. Attia, 2011, "Light-weight key distribution and management for Advanced Metering Infrastructure", IEEE International Workshop on Smart Grid Communications and Networks, 1-5
[7] NIST Interagency Report 7609, 2009, "Cryptographic Key Management Workshop Summary"
[8] H. Debiao, CH.Jianhua, H. Jin, 2011, "An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security", information fusion, vol 13, 223-230
[9] R. Shein, 2010, "Security measures for advanced metering infrastructure components," in Proc. APPEEC, Chengdu, China, 1–3
[10] X. Fang, S. Misra, G. Xue, D.Yang, 2011, "Smart Grid – The New and Improved Power Grid: A Survey", IEEE communications and surveys and tutorials, 1-37
[11] D. Robert, B. Colin, D. Ed, and M. G. N. Juan, 2006, "SKMA—A key management architecture for SCADA systems," in Proc. 4th Austral. Inf. Security Workshop, vol. 54, pp. 183–192.