A Key Management-Based Two-Level Encryption Method for AMI

Imtiaz Parvez, *Student Member, IEEE*; Arif Islam, *member, IEEE;* and Faisal Kaleem , *member, IEEE*

***Abstract* -- In the key management-based security scheme of Advanced Metering Infrastructure (AMI), it is assumed that the established third party and the links between smart meter and the third party are fully trusted. But in wired/wireless communication, man-in-the middle can interfere, and the monitors and controls in the system can expose its vulnerability. Because of this, we propose a security scheme based on two independent and partially trusted but simple servers, which includes two-level encryption without increasing packet overhead. One server (master) manages the data encryption between the meter to ES (energy supplier) and the other server manages randomized data transfer. We also propose a simple node-to-node authentication method based on electromagnetic signal strength.**

***Index Terms* -- AMI, data management, key management, random data, smart meter security, sequential data transfer.**

I. Introduction

Advanced metering infrastructure (AMI) is the distribution-level building block of the smart grid. In AMI, meters collect and report instantaneous consumption data to service provider (SP) periodically rather than having the monthly total consumption recorded in a normal meter. The consumer can observe their consumption history on an allocated website. SP also monitors and controls load demand, tariff and supply, so the communication in AMI is bidirectional. For the network of meters, the communication is proposed in wireless fashion. As the AMI goes into implementation level, security issues emerge with great importance. As with other security requirements [1,8], AMI also requires confidentiality, integrity , availability and accountability (non-repudiation). Confidentiality ensures the privacy of consumers' energy utilization. Integrity requires unaltered data, unauthorized access and control, and reliable communication. Availability requires access to the data and communication network at any time. Accountability ensures timely response to command and control, integrity of the billing profile, etc. However, for small memory and low computational ability in smart meter, complex security schemes cannot be implemented on AMI.

In recent years, the security issues with AMI caught the attention of different communities (electrical engineers, computer scientists, IT experts, etc.), and thus researchers have provided different security schemes. In [2], node-to-node encryption with a dedicated secret key has been proposed. But for a large network, the packet overhead increases in that instance. In [3], several nodes are selected randomly for intermediate node-to-node authentication. Though it reduces the packet overhead, it still has vulnerability during communication. In [4], Costas et al. introduced anonymization of data by a trusted third party (TTP). But it increases communication overhead because TTP needs to communicate with all nodes simultaneously, and it is also very complicated to retrieve information for a large network. In [7], homomorphic encryption has been introduced. In this method, for a large network, data retrieval at the back office (SP) also becomes complicated. In all TTP management systems, it is assumed that the TTP is fully trusted. But the TTP may have been compromised. The same thing may happen for meters and the communication links among TTP and smart meters (SMs). Based on semi-trusted servers and unreliable communication links, we proposed a key management scheme that introduces node-to-service provider encryption as well as random data communication. Our scheme includes two independent servers. The master server manages public key/private key before transmitting meter data using asymmetric encryption. The auxiliary server receives the random sequence of transmitted data in response to public key sent by master server. Both private key, following the public key, and random sequence are used for data retrieval at the service provider office. For node-to-node authentication,

978-1-4799-6415-4/14/$31.00 ©2014 IEEE

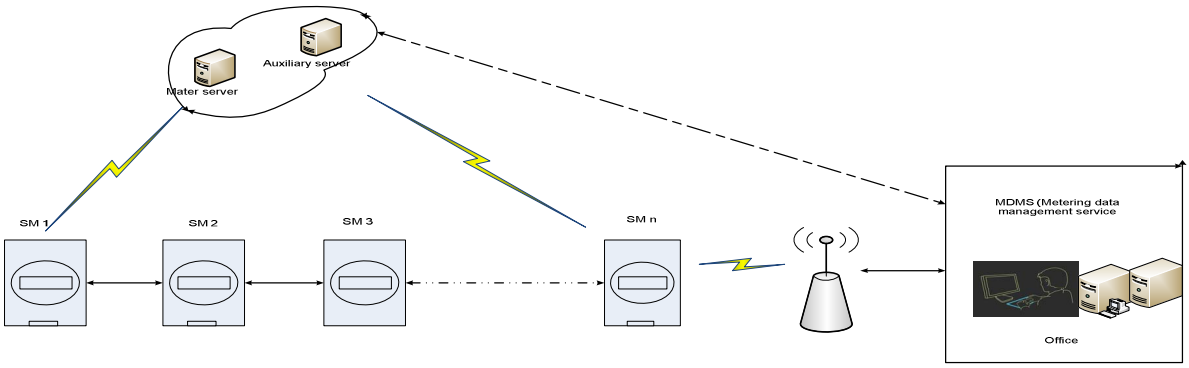

Fig. 1. Network diagram of AMI

the received signal strength (RSS) [10] history has been considered, which is realized in IEEE802.15 communication standard.

The rest of the contents are organized as follows: Section II describes different security aspects of the AMI. In Section III, details of the proposed structure of AMI have been described. Section IV presents the communication and traffic flow among smart meters, servers and the service provider. Furthermore, in Section V, theoretical security strength has been analyzed. Finally, a brief conclusion is included in Section VI.

II. Security Issues of AMI

Because in our model, SMs are connected in a large wireless mesh network like a web network, SMs are vulnerable to various serious cyber-attacks [9-11]. The threats range from threat to consumer's life to blackout in a region. Here, we discuss the threats in the perspective of AMI.

Neighborhood watching/spying: In this attack, man-in-the-middle can listen or monitor the consumer's energy usage profile or pattern and lifestyle from fine-grained data. Also, the attacker can learn whether the target consumer is home or not by viewing the energy usage, which may be a great threat to the consumer's life. Thus unsecured data can reveal the lifestyle of a consumer.

Tampering of packet: The transmitting packets can be trapped, altered and re-sent to the destination. Also, a compromised meter can send false data. An opponent can inject false requests and may flood the network with a large number of packets. The consumers also may want to alter the meter data to reduce their bills.

Compromised node (SM) and keys: A smart meter's information may be hacked. Its identity and secret key may be stolen which can be used in sniffing. It can send false data and may want to control the power supply network. The compromised node (SM) may be able to affect the load demand stability. Also terrorists may perform a blackout in a region via a compromised node (SM).

Jamming of service: The attacker can send a false packet or flood and degrade the service. In a jammed network the utility service provider may lose its control. Also, compromised node may bypass the command from energy service provider (SP). The worst-case scenario for threats is that the attacker could take control of the distribution network, which could lead to a blackout.

III. Structure of AMI

AMI consists of several elements and applications. We can divide the AMI network into three parts: smart meter, communication network and management office (service provider). The elements of the proposed AMI network are described below.

Smart Meter (SM): A smart meter is a solid-state device which can collect, store and send data to SP in less than one hour [8] by using a communication network. SM also implements control command (traffic flow, load demand project, energy supply on/off, etc.) from SP.

Gateway (GW): The gateway is the end node that is connected to SP by a dedicated network. The dedicated network may be PLC (power line communication), optical fiber, intranet, etc. In our model, we assume that the communication between GW and SP is totally trusted.

Service Provider (SP): The service provider receives and records consumption data; makes bills; and also monitors, controls and manages all the meters.

Master Server: We consider the master server to be semi-trusted. It generates a public key and a private key for an SM for each session. The master server unicasts the public key for encryption. The private key is also sent to SP for decryption.

Auxiliary Server: Before encryption of data by public key is sent by the master server, SM generates a random sequence. The random sequence is sent along with public key and secret key of the SM to the auxiliary server. The auxiliary server receives random sequence and authenticates it by SM's secret key and public key.

IV. Traffic Flow Process

In our model, we assume the following:
1) The two servers are mutually independent and semi-trusted. The two servers may be physically one but virtually divided into two servers.
2) The links among servers and meters are not reliable.
3) The SMs have limited memory and computational skills.
4) The service provider (SP) has large computational capability and memory.
5) The meters (SM) keep records of the relative distance of their neighbor SMs based on signal strength.
6) Each node sends data at the same transmitted power.

Initialization: At the beginning of each session, SM1 sends a request to the master server for public key. Master server unicasts public key to that SM1.
Key generation by asymmetric key algorithm [5-6]:

$$A\xi_1 = (k_1, \xi_1, D_1)$$

$$k_1 \xrightarrow{S_1} (\mathrm{p}_{k1}, \mathrm{s}_{k1})$$

Message: The SM1 generates a random sequence (S) and sends it to the Auxiliary Server encrypted with received public key and its own secret key. Using the received public key, the SM1 encrypts the metering data. Furthermore, the SM1 divides the data into a specific number of packets and sends it according the random generated sequence.

Encryption of message: $P_{k1} \oplus M_1 \xrightarrow{S} C_1$

Segmentation: $C_1 \xrightarrow{s} m_1, m_2, m_3, \ldots\ldots\ldots\ldots\ldots m_n$

Order by sequence S:

$$(m_1, m_2, m_3, \ldots\ldots\ldots\ldots\ldots m_n) \xrightarrow{S} (h_1, h_2, h_3 \ldots\ldots\ldots h_n)$$

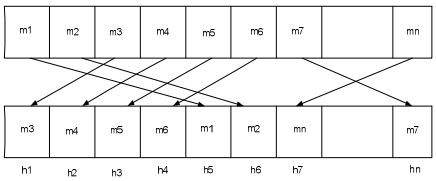

Fig. 2. Ordering the packet according to the sequence

Transmitting Algorithm:

Algorithm

1. Generate Random Sequence (S)

$\lhd sequence, S = (s_1, s_2, s_3 \ldots\ldots s_n)$

2. If Random sequence

$S_{t-1} = !\mathrm{Randomsequence}\, S_t$

3.Do nothing and proceed to next step
4. end if
5. Segment M to m_i

$\lhd m = (\mathrm{m}_1, \mathrm{m}_2, \mathrm{m}_3 \ldots\ldots \mathrm{m}_n)$

6. Assign $P_i = \dfrac{1}{S_i}$

$\lhd P = (\mathrm{p}_1, \mathrm{p}_2, \mathrm{p}_3 \ldots\ldots \mathrm{p}_n)$ where

$$\mathrm{p}_1 = \frac{1}{s_1}, \mathrm{p}_2 = \frac{1}{s_2}, \mathrm{p}_3 = \frac{1}{s_3}, \ldots\ldots\ldots \mathrm{p}_n = \frac{1}{s_n}$$

7. Transmit packet h chosen from

$(h_1, h_2, h_3 \ldots\ldots\ldots\ldots h_n)$ with greater probability $\lhd$ probability distribution

$(p_1, p_2, p_{3\ldots\ldots\ldots}, p_n)$

8.proceed to next step

Fig. 3. Transmitting algorithm for sending packets

Hop-to-hop data aggregation and forwarding: The SM2 calculates the relative distance (R_{12}) between SM1 and SM2 and compares it with the previous record. If the comparison matches, it allows the data and forwards it to the next meter (SM3).

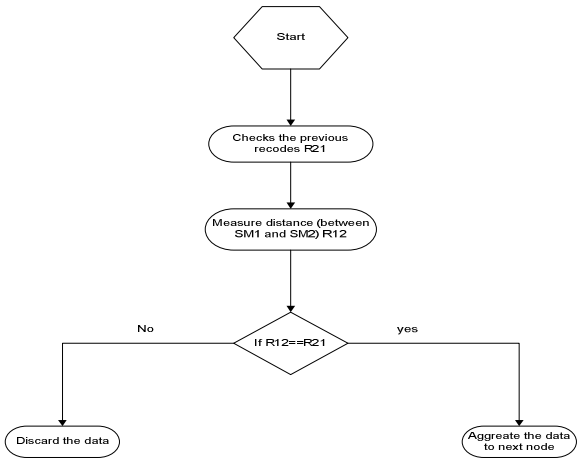

Fig. 4. Flow chart for node- to- node authentication

The SM2 calculates relative distance between it and SM1 by below formula:

$$P_1 - P_2 = L_o + 10\gamma \log_{10} \frac{R_{12}}{d_o} + w \qquad (1)$$

Where, R_{12} is the relative distance between SM1 and SM2, P_1 and P_2 are the transmitted and received power respectively, L_o is path loss at the distance d_o, γ is path loss exponent, and w random Gaussian noise representation.

The probability density of the Gaussian random variable w is given by

$$P(\mathrm{w}) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{(\mathrm{w}-\mu)^2}{2\sigma^2}} \qquad (2)$$

Where w is often modeled as independent and identically distributed Gaussian random variable with zero mean and standard deviation σ.

The electromagnetic signal strength is realized in IEEE 802.15 standard and it is easy to implement.

Data Received: The SP back office receives the randomized encrypted message. We assume this back office has sufficient computational ability.
Reorder of data:

$$(h_1, h_2, h_3 \ldots\ldots\ldots h_n) \xrightarrow{S} (m_1, m_2, m_3 \ldots\ldots\ldots\ldots\ldots m_n)$$

Message unification:

$$m_1, m_2, m_3 \ldots\ldots\ldots\ldots\ldots m_n \xrightarrow{s} C_1$$

Decryption: $C_1 \xrightarrow{s_k} M_1$

V. SECURITY ANALYSIS

Uncertainty is measured by entropy. The more we are certain about a value, the smaller is the entropy.

The entropy for a sequence S:

$$H(S) = \sum_s P(S = s) \log_2 P(S = s) \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Where the $P(S = s)$ is the probability of taking S value over s.

If we generate a sequence S of 32 block with each block size 8, then entropy is 256 (*i.e.* security strength of the random sequence is 2^{256}). For 128 asymmetric key, the security strength is $2^{128/2}$. So for 32 block random sequence and 128 bit asymmetric key, total security strength is $(2^{256} + 2^{\frac{128}{2}})$. So a hacker needs $(2^{256} + 2^{\frac{128}{2}})$ number of operations to decrypt the information, which is impractical.

VI. DISCUSSION

In our key management system, two levels of security have been exerted. For server-to-smart-meter communication, we need bidirectional communication as with meter-data communication. Since the communication between SMs and servers happens once during a session of sending meter data to the SP, it doesn't hamper the normal traffic flow between meters and the SP. Also randomization of packets makes it possible to verify traffic flow from a specific smart meter. Furthermore, electromagnetic signal strength measurement ensures node-to-node authentication.

VII. REFERENCES

[1] Cleveland, F.M. "Cyber Security Issues for Advanced Metering Infrastructure (AMI)", Power and Energy Society General Meeting , IEEE, 2008

[2] Ye Yan ; Yi Qian ; Sharif, H. " A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid " Wireless Communications and Networking Conference (WCNC), 2011 IEEE , 2011 , Page(s): 909 - 914

[3] Ye Yan ; Hu, R.Q. ; Das, S.K. ; Sharif, H. ; Yi Qian "An efficient security protocol for advanced metering infrastructure in smart grid" ," , 2013, Volume: 27, Page(s): 64 - 71

[4]Efthymiou, C. ; Kalogridis, G., " Smart Grid Privacy via Anonymization of Smart Metering Data " ,Smart Grid Communications (SmartGridComm), 2010 , Page(s): 238 - 243

[5] David L chaum, "Untraceable electronic mail, return address and digital pseudonyms".commun, ACM24(2):84-90, 1981

[6] Carbunar, B. ; Yang Yu ; Shi, L. ; Pearce, M. ; Vasudevan, V. " Query privacy in wireless sensor networks "Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on 2007 , Page(s): 203 - 212

[7] Niu Yukun ; Tan Xiaobin ; Chen Shi ; Wang Haifeng ; Yu Kai ; Bu Zhiyong " A security privacy protection scheme for data collection of smart meters based on homomorphic encryption " EUROCON, 2013 IEEE , 2013 , Page(s): 1401 - 1405

[8] Zhou Lu,Xiang Lu,Wenye Wang , Cliff Wang "Review and eavlution of security threats on the communication networks in the smart grid " Military communication conference pp.1830-1835,2010

[9] Mini S Thomas, Ikbal Ali, Nitin Gupta "A secure way of exchanging the secret keys in advanced metering infrastructure"powerCon,2012,pages:1-7 .

[10] Patwari, N., Ash, J.N. ; Kyperountas, S. ; Hero, A.O. ," Locating the nodes: cooperative localization in wireless sensor networks" Signal Processing Magazine, IEEE (Volume:22, Issue: 4), 2006.