Secured Clustered Network for Localization and Monitoring of Smart Energy Meters (SEM) in Ghana

Griffith S. Klogo
Department of Computer Engineering, KNUST, Kumasi, Ghana

James D. Gadze
Department of Electrical and Electronics Engineering, KNUST, Kumasi, Ghana

ABSTRACT
Security of smart energy metering infrastructures is an important issue to address for reliability of sensed data and the authentication and authorization of users of the data. A wireless clustered network has been proposed for the localization and monitoring of smart energy meters. Due to the inability of utility service providers to visit the facilities of consumers regularly results in the difficulty of detecting fraud in good time, when energy meters are tampered with. These tampering, illegal connection and illegal bypass of smart energy meters results in commercial and operational losses. This paper proposes measures to address security issues that may arise in the proposed clustered network for locating and monitoring smart energy meters. The security goals of confidentiality/secrecy, authorization, integrity, authentication and availability and availability that are related to the metering infrastructure are addressed in this paper.

Keywords
Clustered-network, confidentiality/secrecy, authorization, integrity, authentication and availability.

1. INTRODUCTION
The Generation, Transmission and Distribution (T&D) of electricity involves colossal operational losses. The magnitude of these losses is increasing at alarming rates in several countries most especially the developing countries as shown in table 1 [1]. To reduce some of the operational losses at distribution, utility service providers rollout interventions to account for the amount of electricity that eventually gets to the consumer. There is another high percentage loss due to non-technical reasons at customer level such as tampering with the meter, illegal connection and so on. Various attempts have been made to address these worrying problems of non-technical losses such as contracting out meter reading and billing, computerized billing, Smart Energy Meters (SEM) and cut-offs and legal penalties. Automatic meter system (AMR systems) is an aspect of smart grid which is been implemented across the world. In Ghana, AMR systems are gradually been introduced to improve revenue collection and management of power systems by the introduction of smart energy meters in some parts of the country. Unlike traditional energy meters, smart energy meters have wireless communication, sensory, actuating and signal processing capabilities. These smart energy meters can form a network of wireless sensors performing automated metering, demand side management, billing and disconnecting defaulting users remotely. Due to the inadequate planned nature of the countries cities and towns, the meters are not properly monitored to detect fraud and energy theft in good time [2]. To invade paying for power, some customers employ various means such as direct connections, tempering and illegal connections. There is therefore the need to locate the meters remotely and monitor the activities on the meters hence the proposed clustered network shown in figure 1.

Table 1: System Losses from 2002 to 2006 [1]

	2002	2003	2004	2005	2006
Total Purchase in GWh	4,326.29	4,495.96	4,818.05	5,045.40	5,252.84
Annual Increase (%)		3.92	7.16	4.72	4.11
Total Sales in GWh	3,199.75	3,342.87	3,539.40	3,762.03	3,978.41
Annual Increase (%)		4.47	5.88	6.29	5.75
System Losses (%)	26.04	25.65	26.54	25.44	24.26

Ghana is practically new to AMR systems for energy management after relying on the traditional electro-mechanical meters for many decades. In an effort to reduce operational and commercial losses and increase revenue collection, the energy service providers in the country introduced smart (prepaid) energy meter. Following the improvement in the revenue collection in some parts of the country, the smart (prepaid) energy meter are being introduced nationwide [1]. The energy utility service providers and the nation at large stand to gain numerous benefits from the replacement of old electro-mechanical (postpaid) energy meters with smart (prepaid) energy meters. Typical advantages include the convenience of not distributing electricity bills to various household and residence. This will also ensure that tenants do not leave bills to be paid by house owners when the tenants leave the house. The customers also benefit from not having to share electricity bills with co-tenants in the compound housing system typical of most parts of the African sub-region. Despite the advantages to be gained from nationwide installation of smart energy meters, they are still vulnerable to tempering and illegal bypass. Some customers intentionally temper with the meters in an effort to stop the meter from functioning effectively to prolong the usage of the prepaid power. Due to the large number of meters being monitored by the utility service providers, there is the need to structure the meters into groups for effective monitoring. Currently the meters are monitored by the divisional personnel in the

various district offices of the utility service providers. Personnel from the offices of the energy provider occasionally move from door-to-door randomly checking meters to ensure customers are not engaged in any kind of fraud or tempering of meters. To reduce operational cost, a clustered network of smart energy meters as shown in figure 1 is proposed to help locate and monitor activities on the meters remotely. The clustered network even though promises a reduction of operational and commercial losses does raise some security issues that needs to be addressed. Security issues such denial of service attacks, man in the middle attacks and malicious entities having access to data unintended for them. This paper looks at securing the proposed cluster network for locating and monitoring smart energy meters in Ghana. The paper looks at the proposed clustered network for the smart energy meters and the security issues/goals for the network and proposes directions to solving the security challenges in the network.

2. PROPOSED CLUSTERED NETWORK

A cluster is a type of distributed or parallel computer system, which consists of a collection of the interconnected standalone computer working together (by means of some attribute e.g. proximity or location) as a single integrated computing resource [3] [4] [5]. The clustered network for locating and monitoring the smart energy meters is based on the dynamics of the meters and their deployment. The cluster is created base on the received signal strength (RSS) by the Cluster Head (CH) or concentrator. The proximity of the meter to the CH will determine whether it will belong to a particular cluster per its RSS which is a function of frii's transmission equation for free space path loss model satisfying the law of conservation of energy in equation 1 [6]. All CH's are capable of communicating with each other and have routing functionalities as shown in figure 1. The CH also can communicate with the wireless Base Station (BS) in the network.

$$P_r = -32.44 - 20\log(f_{MHz}) - 20\log(R_{km})\ 1$$

Pr = Maximum received power in dB, R = distance of meter from CH and frequency in *MHz* assuming speed of light is $3x10^5 km/s$.

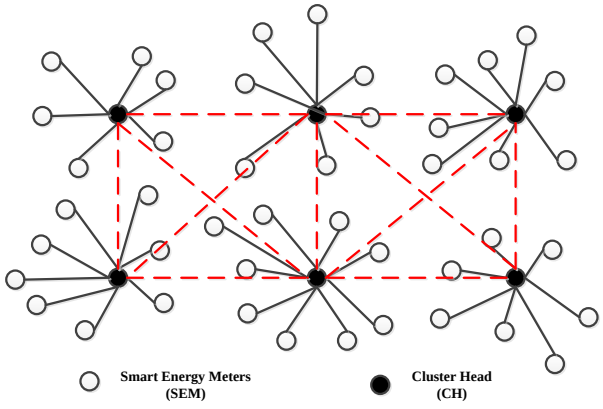

***Fig.1*: Proposed Clustered Network**

2.1 Advantages of clustered SEM network

The proposed clustered network to monitor SEM is informed by the myriad advantages to be derived from implementing such a network. Apart from the benefit of better serving the needs of customers, clustered networks provide;

1. Scalability: By creating small Neighborhood Area Networks (NAN) the energy meters can be monitored remotely to the least level of the network.
2. Simplicity of Network: Scalability means the network becomes simple for both implementation and management. Simplicity to some extent means reduced cost of implementation.
3. Expandability: In a developing country like Ghana, households and residential apartment are always springing up; hence the use of clustered network will enhance effective expansion or addition to the network.
4. Optimized for performance: Clustered networks promote fault tolerance, hence an optimized network that can recover from faults.

2.2 Characteristics of proposed clustered SEM network

The proposed cluster network model for SEM is based on some assumptions, in this paper and for the clustered network model it is assumed that;

1. Each smart energy meters is capable of processing and keeping power consumption into some memory.
2. Each smart energy meters has a communication module, possibly a Radio Frequency (RF) ZigBee device that is standardized by IEEE 802.15.4. Each ZigBee module has a unique 64bits address.
3. There is high level of line-of-sight between the CH and the smart energy meters and there exit a two-way communication between CH and SEM.
4. The CHs are high power, high-memory and high processing energy meters with longer radio signal range than SEM. The CH will usually be a pole-top mounted device to enable wider coverage. The CHs can communicate among each other and the main BS connecting all the clusters for routing and other network function.

2.3 Locating and monitoring SEM

The smart energy meters being monitored collect information that the utility service providers require on regular basis, hence the proposal to use a clustered network to collect this information remotely without necessarily visiting the premise of the customer. This information includes;

1. Location of Meters: The leading energy distribution company in Ghana is currently mapping out the locations of the company's assets including energy meters in the capital city Accra. This is a project that is likely going to be carried out across the nation. With wireless technology and the proposed clustered network, the locations of these meters can be computed and transmitted to data centers of the service providers per query.
2. Performance of Meters: There have been several reports of customer's dissatisfaction with the meters [7]. With remote monitoring via the clustered network, the utility provider will know well in advance the performance of the meters before customers report cases.
3. Consumption History: Meters will regularly communicate their consumption history, which will help the utility service provider to detect irregularity in the case of illegal bypass of meters. Consumption history

will also help utility provider budget for future distribution to particular clusters.

4. Tempering Status: Tempered meters will immediately be communicated to the service provider.

3. SECURITY ISSUES/GOALS

Place There are security issues that immediately come to mind looking at the proposed cluster network. For the clustered network to function effectively there is the need to address these issues that are influenced by the parameters being monitored by the SEMs. There are always malicious people or devices that will want to cause harm to the network for their own interest. Malicious entities are always looking to cause;

1. Denial of service attacks

2. Man in the middle attacks

3. Have access to data unintended for them.

Some of the security goals that can be set for the network include;

3.1 Confidentiality/Secrecy

This ensures that the data's privacy, only sender and receiver can understand the message. This is usually done by the sender encrypting the data and receiver decrypting the data, with a key already known to both communicating party.

3.2 Availability

This ensures reliability of both the network devices in terms of fault tolerance and data being monitored on the network. CH happen to be an essential component in each cluster of the network, hence it has to be fault tolerant in case of denial of service attack on the CH.

3.3 Authentication

Each communicating entity guarantees that it is interacting with the intended party. CH can authenticate the SEM in a one way manner or both CH and SEM authenticate each other to know if they are who they say they are.

3.4 Integrity

Guarantees that the data's content is not modified during transmission.

3.5 Authorization (Access and Capabilities of CH and SEM)

Privileges of all parties on the network need to be clearly assigned to avoid man in the middle attacks.

By meeting these security goals we can assume some high degree of security of the clustered network and the devices of the network, since a system is only secure as and when it is not been breached.

4. SOLUTION TO SECURITY ISSUES

4.1 Authorization

SEM granting access to CH to perform specific task has to be a predefined privilege given to the CH. This is to ensure that a malicious entity or other network devices do not have access to essential service of SEM. The concept of capability list and Attribute Certificate (AC) using symmetric key is explored in the creation of the privileges of the CHs on the network. Each CH keeps its own capability list which will be authenticated by the SEM with the shared symmetric key. The use of symmetric keys does provide fast processing and efficient in power usage. Attributes specify the membership of CHs in the cluster, role(s), security clearance, or other authorization information associated with the AC holder. The AC simply means that the attributes of the holder are inside the certificate. Typical capabilities of CH in interacting with SEM as shown in figure 2 can be;

1. Reading or requesting meters history data (*RD*)
2. Shutting down meter (*Sdown*)
3. Checking meter performance (*Mperf*)
4. Remote update of firmware (*Rup*)

Capability list can be created for the above actions that can be carried out by the CH in interacting with the SEM, since CH has the memory capacity to keep data. Typical capability list (C-list) can be as below,

C-list for CH

$Cap_{(CH)}$: $\{RD, S_{down}, M_{perf}, R_{up}\}$ $\Rightarrow$ Capability list of CH

AC for CH and SEM interaction

$AC_{CH} = CH, Cap_{(CH)}, KPriv_{CA}\{CH, Cap_{(CH)}\} \Rightarrow$ Attribute Certificate of CH

where *CA is a certifying authority*
KPriv is a private key the is issued by a CA

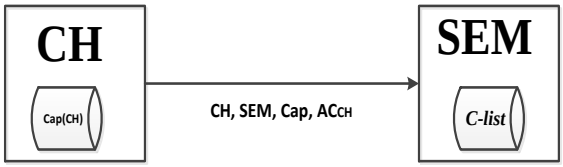

Fig 2: Interaction of CH and SEM using AC

4.2 Authentication

Two-way authentication protocol will be used between the CH and SEM, that is, the CH will authenticate the SEM and vice versa as shown in figure 3. This will ensure that malicious entities will not impersonate either the SEM or CH to cause harm to the network.

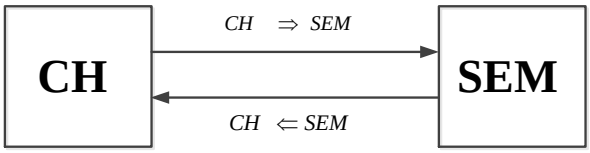

Fig 3: Two-way authentication process of CH and SEM

4.3 Unique Identification

Since each SEM is equipped with a ZigBee module, they can be uniquely identified in the cluster network. ZigBee RF modules have global unique eight byte (8) identification number that can be used to identify each SEM on the network. The unique addresses are used in addition to the RSS from the RF module for the creation of the network in the first place.

4.4 Encryption of Meter Data

Data from the meters and CH will be encrypted using symmetric key that is known to both SEMs and CH on the network [8]. Symmetric key is preferred because it is fast for the SEMs that are limited in terms of processing power [9]. The data from the meters is also hashed with a hashing algorithm to ensure the integrity of the data [9] [10] [11]. The following procedure is used to ensure the integrity and

secrecy of the data using the concept of message authenticating code (MAC) for integrity. Assuming the SEM is transmitting data to the CH. Data and message is used interchangeably.

Data Authentication between SEM and CH

I. *Data (m) is hashed by SEM with a shared key (K_{SEM-CH}) to generate the MAC*

$$SEM \Rightarrow h(m, K_{SEM-CH})$$

II. *The MAC and data (m) are both transmitted to CH.*

$$SEM \Rightarrow m, h(m, K_{SEM-CH}) \Rightarrow CH$$

III. *CH upon receiving the data (m) and MAC also generates its own MAC*

$$CH \Rightarrow h(m, K_{SEM-CH})$$

IV. *CH then compares its MAC to the received MAC to ensure integrity of data (m)*

$$CH_{MAC} = SEM_{MAC}$$

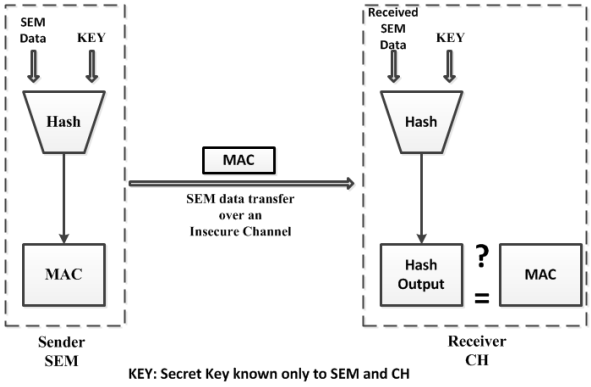

Fig.4: Typical MAC generating process [8]

The above procedure as shown in figure 4 only ensures the integrity of the data but not the secrecy. In other to ensure the privacy of the data the following procedure is used with the same shared key.

Encryption and Authentication of data between SEM and CH

a) *Data (m) is hashed and encrypted by SEM with a shared key (K_{SEM-CH}) to generate the MAC*

$$SEM \Rightarrow h(m, K_{SEM-CH}) \quad , \quad K_{SEM-CH}(m)$$

b) *The MAC and encrypted data (m) are both transmitted to CH.*

$$SEM \Rightarrow \{K_{SEM-CH}(m), h(m, K_{SEM-CH})\} \Rightarrow CH$$

c) *CH decrypts upon receiving the encrypted data K_{SEM-CH} (m) and generates its own MAC*

$$CH \Rightarrow h(m, K_{SEM-CH})$$

$$K_{SEM-CH}(K_{SEM-CH}(m),) \Rightarrow m$$

d) *CH then compares its MAC to the received MAC to ensure integrity of data (m)*

$$CH_{MAC} = SEM_{MAC}$$

5. DISCUSSION OF RESULTS

The proposed solution to the security issues/goals of the metering network will ensure a high degree of security. Making access of the network difficult will increase the cost of overcoming the security measures high, hence a disincentive for the malicious entities. The Attribute Certificate (AC) and the shared symmetric key authorization measure apart from being fast is energy efficient. The interaction between CH and SEM as shown in figure 2, ensures that a third party does not impersonate CH to access functions in SEM. SEM upon receiving the request from CH, checks the validity of the certificate (AC_{CH}) and also check if CH is cleared to access the capability (Cap) then grants access if both the AC_{CH} and Cap are valid. Both CH and SEM have database in memory with the capability list. SEM checks CH's capabilities against its own C-list to confirm what CH is allowed to access in SEM. The two-way authentication of both CH and SEM does provide surety of communicating parties. CH is sure it is communicating with a particular SEM and vice versa as shown in figure 3 and the authentication process between SEM and CH. The encryption of data from both SEM and CH ensures that a malicious entity cannot make meaning of the data when it is intercepted. Using hashing and symmetric key make data encryption and decryption faster and energy efficient.

6. CONCLUSION

The inability of energy distribution companies to detect fraud in good time informed the proposal of a clustered network of smart energy meters for localization and monitoring. This paper evaluated and proposed strategies to address the security issues that may arise in the proposed cluster network. The solutions provided in this paper will be a disincentive for malicious entities to try to overcome the security measures. Security issues/goal of confidentiality/secrecy, authorization, integrity, authentication and availability are addressed in this paper.

7. REFERENCES

[1] Annual Report of Electricity Company of Ghana, 2006

[2] ECG targets 90% prepaid meters for Accra consumers http://thechronicle.com.gh/ecg-targets-90-prepaid-meters-for-accra-consumers/, accessed July 30, 2013, 10:08 GMT

[3] C. S. Yeo, R. Buyya, H. Pourreza, R. Eskicioglu, P. Graham and F. Sommers, "Cluster Computing: High-Performance, High-Availability, and High-Throughput Processing on a Network of Computers"

[4] K. Sun, P. Peng and P. Ning, "Secure Distributed Cluster Formation in Wireless Sensor Networks"

[5] A. A. Abbasi and M. Younis, "A survey on clustering algorithm for wireless sensor networks", Computer Communication 30 (2007) pp 2826-2841

[6] 802.11 Wireless Networks, Security and Analysis, ISDN 1617-7975, Springer London Dordrecht Heidelberg New York.

[7] Consumer Protection, http://www.purc.com.gh/purc/complaints/consumerprotection, accessed July 30, 2013, 18:08 GMT

[8] Secure Socket Layer (SSL) Virtual Private Network (VPN) technology, By Qiang Huang and Jazib Frahim, Network World, October 22, 2008 03:09 PM ET, viewed online http://www.networkworld.com/subnets/cisco/102208-ch2-ssl-vpn-technology.html

[9] White Paper, "Public Key Encryption and Digital Signature: How do they work?" CGI Group Inc., 2004

[10] General Purpose Hash Function Algorithms, http://www.partow.net/programming/hashfunctions/#HashingMethodologies, accessed July 31, 2013, 10:38 GMT

[11] Ayushi, "A Symmetric Key Cryptographic Algorithm ", 2010 International Journal of Computer Applications (0975 - 8887), Vol. 1 – No. 15, pp 1- 4.