A Location based Key Management System for Advanced Metering Infrastructure of Smart Grid

Imtiaz Parvez, Farhan Abdul and Arif I. Sarwat
Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174
Email: {iparv001, fkhay001@fiu, asarwat}@fiu.edu

***Abstract*—In smart cities, Advanced Metering Infrastructure (AMI) is an integral part of utility service which allows automated metering, control and monitoring. Since AMI employs a wireless network for communication, data privacy becomes a burning issue. The attacker can decode the smart meter consumption data, various control commands of components of the smart grid, infuse false command and may even take over the system. Since a smart meter has limited memory and computational capability, we need a light but robust security scheme. In this paper, we propose a location based encryption method where the source node encrypts the data with a key that is associated with its own coordinate points; the destination node receives this data and decrypts it with the key. Since GPS doesn't work inside the multi-stored and in some geographical location like forests, hilly place etc., we propose the localization of source nodes (meters) by Received Signal Strength (RSS) using Maximum Likelihood Estimator (MLE). Finally the strength of security of a data packet is analyzed.**

***Index Terms*—AMI, Data security, Key management system, RSS, Smart meter, Smart grid.**

I. Introduction

In the framework of smart cities, Advanced Metering Infrastructure (AMI) is an important concept which brings automatic metering paradigm using bidirectional communication [1]–[4]. AMI is the distribution level building block of smart grid to deliver electricity to end users with improved monitoring, control and efficiency. Smart meters collect and report the consumption data to the control center of the Service Provider (SP) periodically (typically less than 1 hour) rather than recording the entire monthly consumption observed in conventional meter. It also allows the consumers to engage in electricity trade by selling surplus electricity to the grid. AMI caters to the SP, the control and monitoring with outage management, demand response, disaster prevention and disaster recovery. Consequently, the communication in AMI is essentially bidirectional [5]–[8]. Smart meters and their mesh connected wired/wireless network constituting AMI, being the most imperative aspect of smart grid from the perspective of utility companies as well as the consumers, its assessment and modifications in the current methodology are highly recommended.

Cyber Physical Security (CPS) and reliability of the smart grid have been the points of interest in which a system needs to be designed to detect and prevent an unauthorized access [9]. The attacker may want to decode the data packet, gain control and command over the components of the smart grid, infuse false commands, jam the network, and finally take over the system. Smart meter is the main basis of the collection of consumer usage data through an Access Points (APs). Observing the power consumption and usage pattern of electricity, a thief/attacker can learn the presence or absence of consumers at home and thus posing a greater threat for them.

In 2013, U.S. electric utilities had 51,924,502 smart meter (AMI) installations of which about 89% were residential customer installations [10]. These meters mainly consist of in-built full-duplex communication mode which ranges from periodical reception and transmission of data by instantaneous two way communication. Different solutions for various attacks are proposed based on the usage of electricity in residential areas and security protocols involving various wireless local area network [11]. An experimental setup was performed to analyze the routine usage of electricity corresponding to time of the day. It was observed that the easily identifiable loads such as boilers directly corresponded to the time when laundry, meals and showers were taken. This data can be collected by sniffing or eavesdropping devices and can be used to break into vacant residencies at the time when they are left unattended [12].

Like other systems, AMI needs to fulfill four requirements of security-confidentiality, integrity, availability and accountability (non-repudiation). Confidentiality implies data would be accessible only by the authorized users and any unauthorized attempt would be denied. Since fine grained consumption data of a smart meter conveys consumers life patterns, habits and energy usage, they must be concealed. Integrity requires reflecting authentic data correctly without any modification, addition or deletion. Since the hacker as well as the consumer might want to alter the consumption data, integrity is a vital issue in the AMI network. Availability requirement means that data would be available on demand. Since the hacker or enemy might want to jam the network, the AMI must be comply with availability requirement. Accountability (non-repudiation) means that an entity doing a specific job must not deny it to do that. In AMI, accountability ensures timely responses to the command and control, and integrity of billing profile etc.

In this study, we propose a security scheme to mitigate security threats and capitalize on secured communication

This research was supported in part by the U.S. National Science Foundation under the grant CRISP-1541069 and Presidential fellowship under Florida International University.

978-1-5090-2039-3/16 $31.00 © 2016 IEEE
DOI 10.1109/GreenTech.2016.19

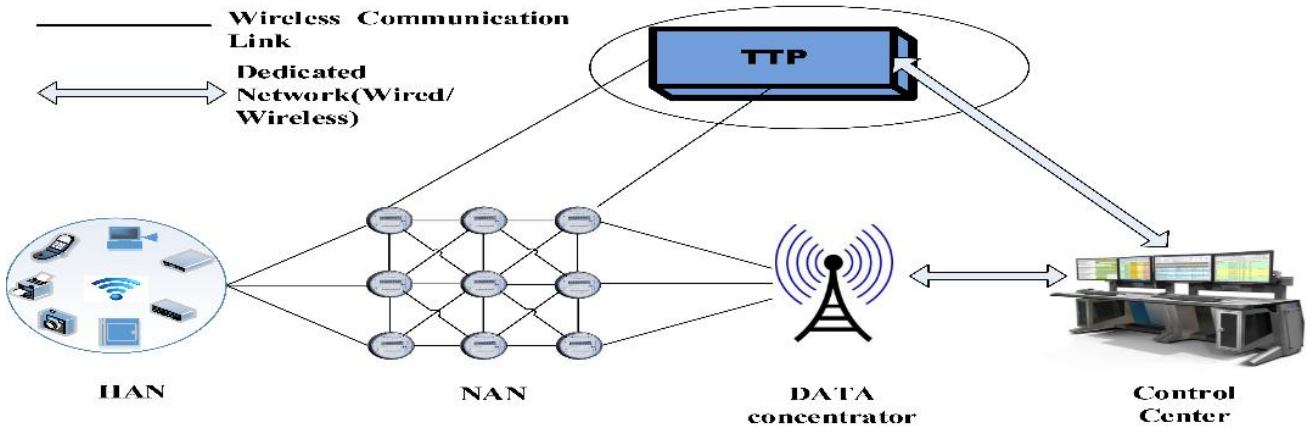

Fig. 1: AMI architecture consists of TTP, HAN, NAN, Data concentrator and Control center.

system by localizing the smart meters, utilizing Received Signal Strength (RSS) of the transmitted Radio Frequency (RF) signal, and data encrypted by secret key associated with the co-ordinate points of the meters. In the GPS based localization, exact position is determined by the signal received from the satellites. Signal from the satellites may be attenuated in some places such as in forests, buildings, hilly areas etc. as well as in multi-stored building. Additionally exact geographic coordinate will contain the location information of meters i.e the consumers which may be exposed. On the other hand, localization by RSS method coordinating with neighbor meters will pinpoint local coordinates with constant error. The derived position is not the exact geographic position of earth coordinate system.

RSS based localization mainly consists of range based technique that utilizes RSS as a reference for distance, and range free techniques which do not use the range factor. In the range based technique, the coordinates of an unknown point are defined exclusively by ranges of a known location. In the conventional Geo-Encryption technique [13], a location based encryption is used to refer to any method of encryption wherein the cipher text can only be decrypted at a specific location. If an attempt is made to decrypt the data at any other location, the decryption process fails and reveals no information about the plaintext. The device performing the decryption determines its location using a form of localization technique based on RSS or other sensors or a satellite or radio frequency positioning system. This technique ensures that the data cannot be decrypted outside a particular facility, for example, a local utility company control center, different government agencies or corporations. In today's signal processing system, any coordinate point can be generated at any place. In our modified scheme, the encryption key is based on coordinate points and a random key index number, and is updated periodically by the system. The encrypted data can be decrypted only with decryption key associated with sender's location and key index number.

The rest of this paper is organized as follows: Section II provides the literature review. In Section III, the AMI architecture has been explained. Section IV elicits the algorithm for localization in details. The simulation results for localizing in residential areas is illustrated in Section V. Security strength of a data packet is analyzed in Section VI. Finally, a brief conclusion is included in Section VII.

II. Literature Review

Data security, being a burning issue of AMI has prompted experts and researchers to provide various security schemes. 128 bit Advanced Encryption Standard Galois Counter Mode (AES GCM) cryptography based security IC is proposed showing a performance comparison between the hardware based and software-based crypto-engines in [11]. Considering an attacker and a defender, an attack level and a severity level, game theory based scheme has been proposed in [12], [14]. Randomly chosen nodes and intermediate authentication among them is proposed in [15]. This process reduces packet overhead, but there is still vulnerability in the middle of the communication. In [16], homomorphic encryption has been introduced. In this method, for a large network, data retrieval at the control center also becomes complicated. In [17], a node-to-node encryption by different secret keys has been proposed. But for a large network, the packet overhead increases because authentication happens at every node. To distribute both the key and manage the network, a wireless sensor network based Public Key management Infrastructure (PKI) has been proposed in [18]. In [13], [19], an encryption key is mapped to longitude, altitude and time for data encryption. In our paper, we propose data encryption associated with latitude, longitude and a random key index. The latitude and longitude are determined by the RSS method.

III. Architecture of AMI

AMI comprises a network of millions of smart meters which are designed to communicate with the local utility service provider and also establish a reliable and firm communication among themselves (as shown in Fig. 1). The

AMI is accountable for periodically collecting, storing and transferring enormous volumes of data packets to the control center through a gateway/data concentrator. Each component of this network has a specific application. A broader aspect of AMI encompasses everything from home appliances to the control center.

Home appliance: Home appliances are day to day machines used at homes, which are electrically powered such as washing machines, dryer, microwave oven, air conditioner etc. These machines consume energy which is calculated per unit of the smart grid system. This unit consumption data is connected to a smart meter which measures and collects the power consumption information.

Smart meter: The smart meter is a crucial part of AMI which is responsible for collecting the consumption unit data from the consumer before sending it to the service provider. Various home appliances are connected to a meter by a network termed as Home Area Network (HAN). Smart meters store, collect and send data periodically through a bi-directional communication network.

Neighborhood Area Network (NAN): The meters communicate among themselves and with the Data concentrator/AP through a mesh connected wired (PLC)/wireless (WiFi, ZigBee, GPRS etc.) network termed as NAN. The back office of SP is connected to the NAN by a wired or wireless connection such as fiber optic or cellular network.

Control center/ Hardware and software control system/ Utility Back office: A bill is issued on the consumer based on the data received from the smart meter. This data is also used in the optimization of the electric power generation and distribution. This also helps in controlling and monitoring of the load from a remote location.

In our model, smart meter, HAN, NAN, control center and TTP will contributed in the security scheme.

IV. Localizing Algorithm and Encryption techniques

A. Localization of Smart meter

In this section, we discuss the localization process of smart meters by RSS method [20]–[22].

Let us assume, there are n partially dispersed known position nodes (smart meters) at positions (x_i, y_i) where $1 \leq i \leq n$ and an unknown node (new smart meter) is at at (x_i, y_i). If the received signal strength at (x_i, y_i) is $\mho_i$, then it follows the model [22]:

$$\mho_i = c - 10\gamma \log_{10}(d_i) + w_i \tag{1}$$

where c denotes a constant dependent on the transmitted signal power frequency.

$\gamma > 0$ is the path loss constant. The generic value of γ is 4-6 from which a value of 2.93 has been used here considering the residential area.

$d_i$is defined as the Euclidean distance between the unknown node and other nodes given by

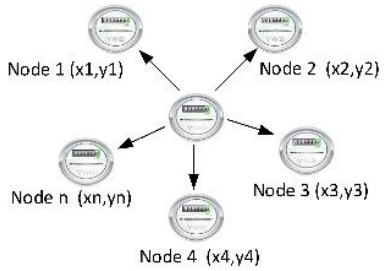

Fig. 2: Localization of new node with known position nodes.

$$d_i = \sqrt{(x - x_i)^2 + (y - y_i)^2} \tag{2}$$

w_i is the zero mean Random Gaussian Noise with known standard deviation σ_i . The typical value of σ is 6 to 12 dB.

We define the θ and $\mho$ as

$\theta = [x, y, z]^T$ and $\mho = [\mho_1, \mho_2, ...\mho_n]^T$

The Likelihood function of θ given an RSS measurement $\mho_i$, $f(\theta/\mho)$ can be written as

$$f(\theta/\mho) = c_1 \exp(-\sum_{i=1}^{n} \frac{(\mho_i - c + 10\gamma \log_{10}(d_i))^2}{2\sigma_i^2}) \tag{3}$$

where c_1 is a constant.

The Maximum Likelihood Estimation of θ denoted by $\hat{\theta}$

$$\begin{aligned} \hat{\theta} &= \arg\max f(\theta/\mho) \\ &= \arg\min\{\sum_{l=1}^{n} \frac{(\mho_i - c + 10\gamma \log(d_i))^2}{2{\sigma_i}^2}\} \end{aligned} \tag{4}$$

The ML estimation of an unknown node's location (x, y) based on the RSS measurement $\mho_i$ using optimization technique, can be written then as:

$$(x_r, y_r) = \{\hat{\theta}(1)), \hat{\theta}(2)\} \tag{5}$$

V. Encryption process

In this section, we describe the entire encryption and data flow process of AMI in detail. Before we proceed to the steps of encryption and data flow, the assumptions are outlined in the below:

Assumptions:

1) The meter has a limited memory and computational capability.
2) The control center has sufficient computational capability.
3) Every meter holds records of the location of its neighboring meters.
4) Every meter transmits data at a constant power.
5) There is a codebook that has an encryption key associated with each coordinate point of the geo location (as illustrated in Fig. 3).

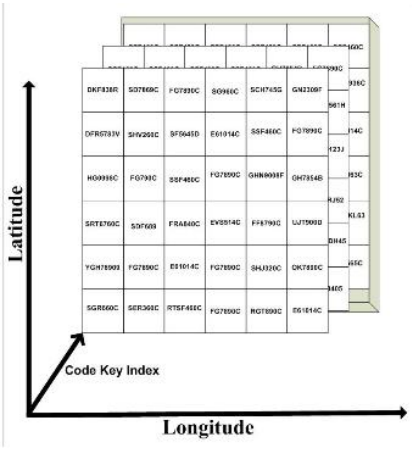

Fig. 3: Mapping of encryption key based on coordinate point.

6) The Trusted Third Party (TTP) updates the codebook associated with geo-location /co-ordinate point periodically.

Initialization:

For each session of data transmission, the source meter initiates the process and chooses a key index randomly. The key index is encrypted by node ID and sent to TTP. The TTP identifies the node and send the random key index to the control center.

Data Encryption:

In this step, the meter encrypts the consumption data text with the corresponding encryption key associated with its own co-ordinate point (location) and key index.

Encryption:

$$k_1 \oplus m_1 \longrightarrow C_1 \tag{6}$$

Data forwarding and authentication:

The encrypted message is forwarded to its neighboring meter. Getting packet, it determines the location of the source meter and compares it with the previous records. The authenticated packets are forwarded to next neighboring meter. In this way, the packets are relayed and finally reach the control center of the energy service provider, which is described in pseudo algorithm I.

De-encryption:

The control center receives data and decrypts them with the help of the key associated with the location of the meter and an index key.

Decryption:

$$C_1 \longrightarrow m_1 \tag{7}$$

VI. Simulation result

To evaluate the performance of the localization of meters, we use rectangle, hexagon and octagon shaped Area Of Interest (AOI) (with approximate dimension of $10m \times 10m$) as shown in Fig. 4 . Each edge represents a known position

Algorithm 1 Transmitting algorithm

1: **Initialization:**
2: Derive position of neighbor meter by RSS method at time instant $t = 0$
3: Calculate and record distance between source meter and neighboring meter $R_{i,j}(0) \forall i, j \in M$
4: **Data forward:**
5: For each packets, drive position of source node
6: Calculate distance between current node (meter) and source node (meter) $R_{i,j}(t)$
7: **if** $R_{i,j}(t) == R_{i,j}(0)$ **then**
8: Forward data to the next node
9: **else**
10: Discard the data
11: **end if**
12: **End**

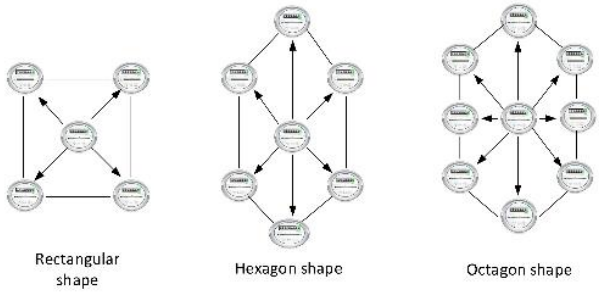

Fig. 4: Different shapes of AOI.

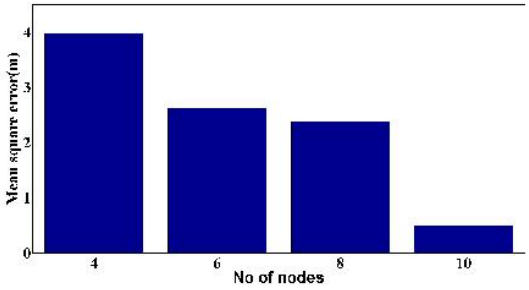

Fig. 5: No of Nodes vs Mean square error(m).

node (meter), and the emitter (unknown node/meter) is the center of the AOI. The estimation of position of the unknown meter (emitter node) through equation (1) is the optimization problem. In our simulation, we used the Particle Swarm Optimization (PSO) method.

In the Fig. 5, we observe that with an increase of the number of the nodes, the mean square error from the exact position will decrease. At the same time, with an increase of the path loss constant, the mean square error will decrease as illustrated in fig 6.

In the path loss model of radio signals, random noise is added which varies by standard deviation. In the Fig 8, the

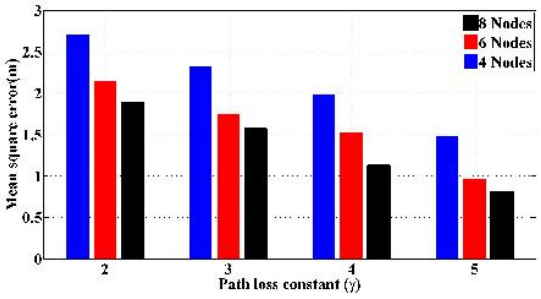

Fig. 6: Path loss vs Mean square error(m).

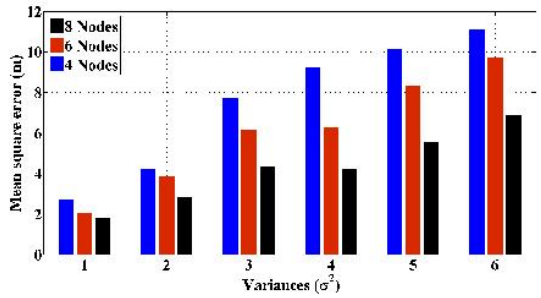

Fig. 7: Variance vs Mean square error(m).

error curve is drawn as a function of variance for different number of nodes. As the variance of the noise increases, the error also hikes correspondingly. So the more is the variance, the more error will be added in determining the position of unknown meter.

VII. Security strength analysis

The security strength of a data packet can be measured by Entropy. The value of Entropy reflects the uncertainty of a random variable. The more certain about a value is, the smaller the entropy value.

The entropy for a sequence S [23]

$$H(s) = \sum_S P(S = x) \log_2 P(S = x)$$

where $P(S = x)$ is the probability of taking S value over x.

Let us consider, a smart meter sends a data packet of 128 bit encrypted by 128 bit symmetric key to control center. For a 8 bit random key index, the security strength of the random sequence is 2^8. On the other hand, for a 128 bit symmetric key algorithm, the security strength is 2^{128}.

So, for a 8 bit random key index and 128 bit symmetric key,

The security strength of the packet= $2^8 + 2^{128}$

So, if a hacker wants to decrypt a data packet of 128 bit, he needs $(2^8 + 2^{128})$ number of tries to decrypt the message. This is impractical.

VIII. Conclusion

In our scheme, we use the encryption key corresponding to meter's location. The codebook relating the encryption code to its geographical location can be updated periodically in a secured way by the TTP. Since the same code book is used for all smart meters, it will invalidate the need for using different keys for different meters each time. Also the location of smart meters will be determined by the MLE which is nearly constant due to fixed power transmission and stable positions of meters. This increases the stability and security of the smart grid system without potential hackers intervening the data manipulation.

An automated, secure and reliable metering paradigm is an essential component for the designing and building smart cities with high standards of living and providing vibrant socio economic climates to the citizens. Since fine grained data of meters contain important information about the consumers, revealing the data compromises the citizen's privacy. Our paper proposes a technique to resolve a fraction of smart grid security threats and making the communication more secure and reliable.

References

[1] S. Karnouskos, P. Da Silva, and D. Ilic, "Energy services for the smart grid city," in *Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference on*, June 2012, pp. 1–6.

[2] N. C. Tse, J. Y. Chan, and L. L. Lai, "Development of a smart metering scheme for building smart grid system," in *Advances in Power System Control, Operation and Management (APSCOM 2009), 8th International Conference on*, Nov 2009, pp. 1–5.

[3] Q.-D. Ho, G. Rajalingham, and T. Le-Ngoc, "Performance and applicability of geographic-based routing in smart grid's neighbor area networks," in *Advanced Technologies for Communications (ATC), 2013 International Conference on*, Oct 2013, pp. 215–219.

[4] I. Parvez, F. Abdul, H. Mohammed, and A. I. Sarwat, "Reliability assessment of access point of advanced metering infrastructure based on bellcore standards (telecordia)," in *SoutheastCon 2015*, April 2015, pp. 1–7.

[5] I. Parvez, A. Sundararajan, and A. Sarwat, "Frequency band for HAN and NAN communication in Smart Grid," in *Proc. on IEEE Sym. on Computational Intelligence Applications in Smart Grid (CIASG)*, Dec 2014, pp. 1–5.

[6] F. Granelli, D. Domeniconi, N. da Fonseca, and B. Tsetsgee, "On the Usage of WiFi and LTE for the Smart Grid," in *Proc. Int. Conf. on Ubi-Media Computing and Workshops (UMEDIA)*, July 2014, pp. 1–5.

[7] I. Parvez, N. Chotikorn, and A. I. Sarwat, "Average Quantized Consensus Building by Gossip Algorithm using 16 Bit Quantization and Efficient Data Transfer Method," in *International conference on Intelligent Systems, Data Mining and Information Technology (ICIDIT)*, 21-22 April 2014, pp. 1–5.

[8] J. Brown and J. Khan, "Performance analysis of an LTE TDD based smart grid communications network for uplink biased traffic," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec 2012, pp. 1502–1507.

[9] I. Cavdar, "A solution to remote detection of illegal electricity usage via power line communications," in *Power Engineering Society General Meeting, 2004. IEEE*, June 2004, pp. 896–900 Vol.1.

[10] Independent statistics and analysis. [Online]. Available: http://www.eia.gov

[11] W. Somkaew, S. Thepphaeng, and C. Pirak, "Data security implementation over zigbee networks for ami systems," in *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2014 11th International Conference on*, May 2014, pp. 1–5.

[12] Z. Ismail, J. Leneutre, D. Bateman, and L. Chen, "A game theoretical analysis of data confidentiality attacks on smart-grid ami," *Selected Areas in Communications, IEEE Journal on*, vol. 32, no. 7, pp. 1486–1499, July 2014.

[13] D. Scott, L.and Denning, "A location based encryption technique and some of its applications," in *National Technical Meeting of The Institute of Navigation*, vol. 4, Jan. 2003, pp. 734–740.

[14] S. Amin, G. Schwartz, A. Cardenas, and S. Sastry, "Game-theoretic models of electricity theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure," *Control Systems, IEEE*, vol. 35, no. 1, pp. 66–81, Feb 2015.

[15] Y. Yan, R. Hu, S. Das, H. Sharif, and Y. Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," *Network, IEEE*, vol. 27, no. 4, pp. 64–71, July 2013.

[16] N. Yukun, T. Xiaobin, C. Shi, W. haifeng, Y. Kai, and B. Zhiyong, "A security privacy protection scheme for data collection of smart meters based on homomorphic encryption," in *EUROCON, 2013 IEEE*, July 2013, pp. 1401–1405.

[17] Y. Yan, Y. Qian, and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid," in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, March 2011, pp. 909–914.

[18] R. Bhatia and V. Bodade, "Defining the framework for wireless-ami security in smart grid," in *Green Computing Communication and Electrical Engineering (ICGCCEE), 2014 International Conference on*, March 2014, pp. 1–5.

[19] M. Firoozjaei and J. Vahidi, "Implementing geo-encryption in GSM cellular network," in *Communications (COMM), 2012 9th International Conference on*, June 2012, pp. 299–302.

[20] S. Wang, R. Inkol, and B. Jackson, "Relationship between the maximum likelihood emitter location estimators based on received signal strength (RSS) and received signal strength difference (RSSD)," in *Communications (QBSC), 2012 26th Biennial Symposium on*, May 2012, pp. 64–69.

[21] R. Vaghefi, M. Gholami, R. Buehrer, and E. Strom, "Cooperative Received Signal Strength-Based Sensor Localization With Unknown Transmit Powers," *Signal Processing, IEEE Transactions on*, vol. 61, no. 6, pp. 1389–1403, March 2013.

[22] I. Parvez, M. Jamei, A. Sundararajan, and A. Sarwat, "RSS based loop-free compass routing protocol for data communication in advanced metering infrastructure (AMI) of Smart Grid," in *Computational Intelligence Applications in Smart Grid (CIASG), 2014 IEEE Symposium on*, Dec 2014, pp. 1–6.

[23] I. Parvez, A. Islam, and F. Kaleem, "A key management-based two-level encryption method for AMI," in *PES General Meeting — Conference Exposition, 2014 IEEE*, July 2014, pp. 1–5.