GELİŞMİŞ ÖLÇÜM ALTYAPISI İÇİN GÜVENLİK UYGULAMALARI
SECURITY PRACTICES FOR ADVANCED METERING INFRASTRUCTURE

Elif Üstündağ Soykan[1], Seda Demirağ Ersöz[1]

1. TÜBİTAK, BİLGEM, UEKAE
{elif.ustundag, seda.ersoz}@tubitak.gov.tr

ÖZETÇE

Elektrik tüketimi ölçüm araçları, manuel olarak ölçüm yapılan analog sayaçlardan, elektrik tüketimi ile ilgili bilgileri toplayan ve elektrik dağıtım firmalarına ileten yeni akıllı sayaçlara doğru evrilmektedir. Sayaç verisinin okunmasını sağlayan tek yönlü otomatik sayaç okuma sistemlerinin (AMR) çıkışıyla sayaçlar akıllı şebeke yatırımlarının önemli bir kısmını oluşturmuştur. Otomatik sayaç okuma sistemleri ilk uygulamalar için cazip olmasına rağmen, çözülmesi gereken önemli bir husus olan talep tarafı yönetiminin AMR ile sağlanamadığı fark edilmiştir.

AMR teknolojisinin kabiliyetlerinin tek yönlü sayaç verisi okuma ile sınırlı olması nedeniyle, sayaçlardan toplanan veriler üzerinden düzeltici önlemler alınmasına ve tüketicinin enerjiyi daha verimli akıllı kullanmasına yönelik özeliklere izin vermemektedir. Gelişmiş Ölçüm Altyapısı (AMI) ise akıllı sayaçlar ve dağıtım şirketleri arasında çift yönlü iletişim kurarak dağıtım şirketlerine sayaçlar üzerindeki parametreleri dinamik olarak değiştirme imkanı tanır. Bu nedenle, bu çalışmada AMI güvenliği üzerine odaklanılacaktır.

Akıllı sayaç sistemlerinin yaygınlaşması ile birlikte, güvenlik bu sistemlerin gerekli ve kaçınılmaz bir ihtiyacı haline gelmektedir. Diğer taraftan, AMI sadece akıllı sayaçların fiziksel olarak dağıtımı manasına gelmemekte, ayrıca sayaç verilerinin yönetimi için gerekli olan karmaşık bir iletişim ağı ve bilgi teknolojileri altyapısını da içermektedir. Dolayısıyla güvenlik çözümlerini ele alırken geniş bir perspektifle yaklaşmak gerekmektedir. Bu nedenle de, sistemin kritik varlıkları belirlenmeli, tehditler iyi analiz edilmeli ve daha sonra güvenlik gereksinimleri iyi tanımlanmış olmalıdır.

Bu çalışma AMI sisteminin temel güvenlik gereksinimleri, tehditlere karşı sistem kısıtlarını düşünerek olası çözümleri üzerine, şu anki güvenlik çözümlerini de resmederek, genel bir bakış sunmaktadır. Bu çalışmada, AMI sisteminin güvenlik gereksinimleri analiz edilecek, kısıtlar belirlenecek ve olası güvenlik tehditlerine karşı olası karşı önlemler belirlenecektir.

ABSTRACT

Metering utilities have been replacing from analog meters that are read manually with new, smart meters that gather information about electricity consumption and transmit it back to electric companies. The metering has been the important part of the Smart Grid investments so far, with the initial introduction of one-way automated meter reading (AMR) systems to read meter data. Even though AMR technology proved to be initially enticing, utility companies have realized that AMR does not address demand-side management which is the major issue they need to solve.

Since AMR's capability is restricted to reading meter data due to its one-way communication system, it does not let utilities take corrective action based on the information gathered from the meters and does not assist customers in using energy intelligently. Advanced Metering Infrastructure (AMI) creates a two-way communication network between smart meters and utility systems and provides utilities the ability to modify service-level parameters dynamically. Therefore in this work we will also focus on AMI security practices.

While smart metering systems are become widespread security is going to be the one of its essential and inevitable needs. On the other hand, AMI does not only mean the physical deployment of smart meters, but it also includes meter data management system which is a complicated communication network and IT infrastructure. Hence a broad perspective has to be adopted when security solutions are considered. Therefore, assets of the system must be identified, threats must be well analyzed and then security requirements must be well defined.

This paper presents an overview on the main security requirements of the AMI, on the threats possible solutions considering the system constraints by picturing the current security solutions. In this work, the security requirements for AMI systems will be analyzed, constraints will be determined and possible countermeasures against security threats will be given.

1. INTRODUCTION

Smart Grid is used to enhance the efficiency of electricity usage and the communication among power generation, transmission and distribution systems. As a new emerging technology for smart grid, advanced metering infrastructure (AMI) system used to measure, collect, store, analyze, and use energy usage data. It provides a bridge between consumers and electric power utilities. The AMI is also responsible for transmitting requests, commands, pricing-information and software updates from the authorized parties to the smart meters. In the future utility companies will deliver energy and information to customers through a "smart" energy supply chain created by the convergence of electric, communication and information technologies [17].

There are considerable numbers of benefits switching to AMI from the conventional energy distribution systems. From electric power utility companies point of view, AMI provides the ability of performing remote meter reading, remotely detecting power outages, performing remote diagnostics, accommodating variable power generation and storage option and finally offering more prepaid options to customers. AMI ensures a better awareness of their energy usage, improved power quality, accurate billing and resolution of power failure issues for the customers. Also by using AMI, customers can make and execute intelligent decisions reading energy consumptions and storage [3].

As the AMI becomes reality, security threats from inside and outside of the system grow exponentially. For utilities, there is a high possibility of facing liability claims and regulatory fines if inadequate security technologies enable attackers to acquire and use AMI data. In addition, if customers think that a utility is abusing personal data, or is generally collecting information beyond what they assume acceptable, then they are likely to resist the implementation of AMI. Consumers may refuse to give permission, hide their data or pursue political opposition. Therefore, confidentiality for user privacy and meter data and authentication for meter reading and configuration messages, are two of the major security services need to be provided by AMI security architecture [9].

In this work, firstly, an overview for AMI architecture will be given. After then, possible security threats and security requirements for the AMI will be discussed. Finally, based on these security requirements, appropriate security solutions will be given by considering the AMI constraints.

1.1. AMI Communication Architecture

The AMI system is not responsible only for collecting, analyzing, storing the metering data sent by the smart meters but also responsible for transmitting commands, pricing-information and software updates to the smart meters. From the communication point of view, AMI system consists of the following components: Home Area Network (HAN) which is the network of smart home appliances, the smart meter which is source of measured data, data collector unit which is responsible for aggregating data sent from smart meters, wide area network which is a two way communication network that connects Data Collector Units and Data Management Center (DMC) and finally DMC that interacts with data collector units to handle metering data and also focuses on business application such as CRM, billing or payment systems. The given AMI infrastructure is represented in Figure 1.
The vision for HANs is to connect the smart meter, smart appliances, electric vehicles, and on-site electricity generation, both for in home displays, data uploads, and to allow control of energy loads during peak demand periods. The communications needs of on premises applications are generally handled by low power, short distance wireless technologies. Technologies currently being used for HAN communications include 2.4 GHz WiFi, the common 802.11 wireless networking protocol, ZigBee, which is based on the wireless IEEE 802.15.4 standard and HomePlug, a form of power line communications (PLC) that carries data over the existing electrical wiring in the home.

Smart meters are connected to a Data Collector Unit, which acts as a gateway and is responsible for aggregating data sent from smart meters and transmits it to the DMC. For the smart meter Data Collector Unit communications, early AMI installations used narrowband PLC technology, which is used for relaying meter data and other internal communications over a utility's power lines. Even though traditional PLC is narrowband, it is still the common transmission line for AMI functions in rural areas, where wireless coverage is less available[18]. Also, many AMI deployments, particularly in urban areas, use 900 MHz wireless mesh networks. For the higher throughput needs, broadband communications such as the IEEE 802.16e mobile WiMAX standard, broadband PLC, or next generation cellular technologies are the alternatives of the already mentioned technologies.

Since the amount of metering data is growing dramatically due to the millions of communication between smart meters and utilities' headend, the inevitable requirement of an AMI is the DMC. The DMC is responsible to collect and analyze metering data for further dynamic pricing, better customer service, outage management, demand response and energy consumption management purposes [5]. The backhaul of information from data collection points to the DMC typically functions over WAN which can be accomplished using a variety of technologies, such as Ethernet, fiber, T1, or commercial wireless networks [18].

2. SECURITY THREATS

Lack of Integrity: Integrity for AMI systems means not only preventing changes to data as it is retrieved from the meter, but also the integrity of control commands, such as preventing unauthorized control commands from being transmitted through the AMI system to the smart meter or data collector unit since AMI network is open to external, unsecured environments [1].
Lack of integrity may result in modification of the commands sent from the AMI DMC by attacker that change pricing signals, request load control actions, to reset meters, or to connect/disconnect loads and distributed generation.

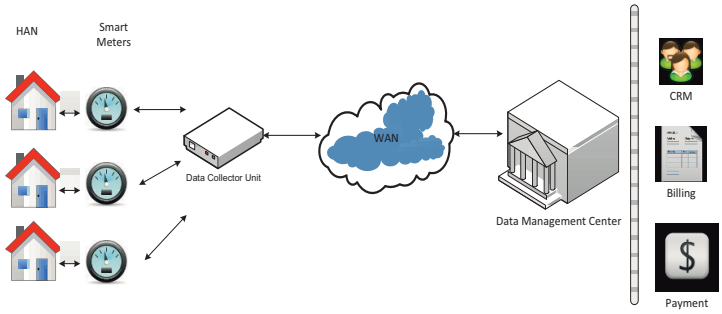

Figure 1: Communication architecture of AMI

Lack of Confidentiality: Confidentiality requires that only the sender and the intended receiver should understand the contents of a message. Confidentiality is needed to protect privacy at the customer site. Customers do not want unauthorized people or marketing firms to know how much energy they are using, how their signature of energy usage is. Utilities may also not want other competing utilities access their offers, activities or related information. Therefore, communication in AMI network must be held confidential, including preventing the physical theft of meters for subsequent access to the stored data.

Lack of Authentication: The identity and legality of the smart meters and associated consumers should be verified before joining the interconnected smart meter network and receiving proper utility service. However, authentication processes can be manipulated by an adversary to impersonate legitimate devices or expose systems to denial of service conditions When the field tools is used without performing authentication before gaining access, unauthorized entities become able to gather information about customers energy usage [4].

Lack of Replay Protection: Some cryptographic primitives accept received data as valid after checking that the data decrypts properly. However, without additional verification functions such as sequence counting, the protocol will be vulnerable to replay attacks, where an attacker can listen a valid encrypted data and retransmit it. An attacker can identify systems vulnerable to replay attacks by identifying the lack of unique identifiers in each cryptographic frame, or by observing repeated ciphertext content transmitted by one or more sources [6].

Crypto Related Flaws: Improper use of cryptography may enlarge the attack surface by giving attacker additional oracles.

In stream ciphers, key stream data cannot be re-used without unsecuring the confidentiality of the cryptosystem. By implementation mistakes, having reused key stream data allows an attacker who observes a plaintext/ciphertext pair to recover the plaintext of an unknown ciphertext value.

While some encryption algorithms are considered secure, the use of an insecure mode such as Electronic Codebook (ECB) can threaten the security of the cryptosystem allowing an attacker to deduce repetitions plaintext content from repeated ciphertext blocks.

The use of weak integrity check functions allow an attacker to manipulate ciphertext data, allowing them to selectively modify data while preserving a valid integrity check value (so called "bit flipping" attacks), and may cause AMI system to accept unwanted command or data without realizing the alteration. It would be a disaster a hacker issuing disconnect commands to millions of meters because there was a weak integrity control or no way of checking at all of these commands.

Encryption algorithms may provide insufficient protection against an attacker if key length is not long enough. This is most notable in symmetric ciphers such as the Data Encryption Standard (DES). On the other hand, without sufficiently randomness for key generation, all keys used by the algorithm are suspect, allowing an attacker the ability of guessing keys and decrypting data or impersonating trusted devices.

Key Management: Even though the communication encrypted, extracting the encryption key from meter could be demonstrated if keys are not stored in a secure module or no anti-tamper mechanism is implemented. Hence, using the same encryption key on a large number of devices raises a system wide security problem; because when a potential attacker discovers this single key he could take over a large number of smart meters [16]. Therefore avoiding symmetric cryptographic mechanisms and choosing asymmetric crypto would be a good practice.

Design and Implementation Flaws: Design security flaws are made at multiple levels of the device design, including chip design, firmware, protocol, usage etc. For example, a communications protocol which allows access to key elements of the meter without authentication would be considered a design flaw [6]. Implementation flaws are vulnerabilities which are caused by programming mistakes. These vulnerabilities are most commonly the results of programmers failing to consider or to understand the full impact of their code. The well-known implementation attack is called buffer overflow which is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory [19]. There are many causes of buffer

overflows, most of which are made possible by the abuse of API calls.

3. SECURITY REQUIREMENTS

The National Institute of Standards and Technology (NIST), Open Smart Grid (OpenSG) and some other organizations are working for identifying the security requirements of AMI in order to safely integrate the smart grid technology into the power grid system [15].In this section we give an overview of the security requirement not only network security point of view but also information system security point of view.

Confidentiality: The AMI system design and implementation shall protect the confidentiality of the communication where necessary. The information transmitted in an AMI system may have confidentiality requirements because it must ensure the privacy of customer and business information. The confidentiality requirements can be violated both intentionally and unintentionally and can lead to system instability, malfunction, privacy violation, loss of business advantage, and a host of other impacts. The confidentiality requirement should be implemented such that the latency introduced by security functions shall not affect the performance or degrade the functionality.

Integrity: The AMI security architecture shall protect the integrity of meter data and control and configuration commands being altered without detection. The AMI security architecture shall employ cryptographic mechanisms for ensuring detect of changes in information transmitted. It is important to use cryptographically strong integrity mechanisms since weak algorithm may cause vulnerabilities as mentioned earlier.

Availability: AMI security architecture shall ensure that data and systems are up and operational when they are needed. AMI components shall protect against or limit the effects of denial-of-service attacks. The AMI system should restrict the ability of internal or external users to launch denial-of-service attacks against other AMI components or networks. The AMI system should manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks. Wireless assets and networks are also vulnerable to radio-frequency jamming and steps should be taken and personnel trained to address tracking and resolution of such issues. If communication within the AMI system relies on a name/address resolution service then it shall be designed and protected to provide sufficiently reliable services. The utility shall monitor address resolution traffic to identify potentially malicious patterns of behavior.

Device Identification and Authentication: The AMI system shall employ a mechanism to identify and authenticate specific components before establishing a connection. Device authentication is a common layer of defense and presents a hurtle that attackers shall overcome before gaining access to a system. This also prevents attackers from gaining access to the AMI system by spoofing existing devices.
The authentication mechanisms in the AMI component/system shall obfuscate feedback of authentication information during the authentication process to protect the information from possible exploitation by unauthorized individuals. This applies to authentication by one component to another as well as by individuals. This control blocks several known attacks to user authentication including user enumeration, cached form field extraction, authentication sniffing, and brute force optimizations [8].
AMI devices are able to support lightweight automatic authentication mechanism which is suitable for embedded system. Moreover, mutual authentication between devices is required for efficient network configuration because there is hierarchy dependency on network configuration between DMC and meter. It cannot be obtained using existing authentication protocol like Kerberos because meter cannot communicate with authentication server without passing through DMC.

Access Control and Access Control Management: The security architecture shall provide security measures to restrict access and input to the AMI system to authorized personnel only. All communications between AMI components shall be authenticated.
The AMI components with user interfaces shall limit the number of consecutive invalid attempts by a user during a given time period. The component disables user accounts when the maximum number of unsuccessful attempts is exceeded and logs all unsuccessful login attempts.

If password based authentication method is employed**,** passwords shall not be embedded into tools, source code, scripts, aliases or shortcuts. It is the fact that many AMI components and software are shipped with factory default authentication credentials to allow for initial installation and configuration. In these case default password must be changed before deployment of the component since factory default authentication credentials are often well known, easily discoverable, present a great security risk.
For symmetric/password-based authentication, the AMI system [17]:

- Shall protect passwords from unauthorized disclosure and modification when stored or transmitted;
- Shall prohibit passwords from being displayed when entered;
- Shall enforce password lifetime restrictions;
- Shall employ counter for maximum number of unsuccessful attempts.

For asymmetric/PKI-based authentication, the AMI system [17]:

- Shall validate certificates by constructing a certification path to an accepted trust anchor;
- Shall enforce authorized access to and use of the corresponding private key;
- Shall map the authenticated identity to the user account.
- Shall restrict field tools password and keys life-span in case they are stolen.

Key Management: AMI security architecture shall provide management policies of keys such as key generation, distribution, renewal and revocation. Successful key management is critical to the security of a cryptosystem. Even if you design the most secure system, a security breach in the key management such as outdated keys, lack of revocation mechanism or the careless personnel who is the weakest link would ruin whole system. Key management considered as the most difficult aspect of cryptography because it involves system policy, user training, organizational and departmental interactions, and coordination between all of these elements [8].

Security Services and Protocols: AMI security architecture shall provide controlling and monitoring protocols and services. All allowed protocols and services should be identified and explicitly authorized with all others being filtered out of the system and denied all access that is white listing approach.

Malicious Code Protection: From a system perspective, malicious code protection mechanisms shall be deployed in such a manner as to limit the impact of the attack to a small geographical area prior to detection and termination. These include critical entry and exit points between HAN, meters, aggregation points and WAN.
The AMI meter should ensure that no malicious code can pass from the consumer's HAN to the utility's network.
Cyber Security Related Requirements: All components of the AMI system or any device connected to the AMI network shall employ host hardening, including patch application and security concerning configurations of the operating system, browsers, and other network related software. [7].
Intrusion detection systems shall be installed within each network segment with event monitoring / event response and subsequent prevent for incoming and outgoing network traffic, including anti-virus, anti-spyware and signature and anomaly-based traffic monitors [7]. It is also highly recommended that an AMI network be appropriately isolated from any general-purpose enterprise networks as they can introduce risks. Access Control Lists shall be employed at all points which bridge data collector segments to WAN to limit incoming and outgoing connections to only those necessary to support the AMI system [7].
All firmware/software shall be checked against malwares and viruses prior to loading on any component of the AMI system or device connected to the AMI network. Smart meters or data collector unit shall not allow uploading of any executable code from the consumer's HAN [7].

Field Tools: The utility shall use approved and certified field tools. Utility is responsible to manage, protect, and monitor the use of field tools and shall maintain the integrity of these tools on an ongoing basis. Field tools also represent a potentially higher risk due to their portability and likelihood of being connected to numerous networks. If not properly secured and controlled, they can be a mechanism to bypass security controls and allow malicious code to be transported from one security zone to another.

Remote Maintenance: The DMC shall authorize, manage, and monitor remotely executed maintenance and diagnostic activities of the AMI system. The utility shall audit all remote maintenance and diagnostic sessions and authorized personnel review the maintenance records of the remote sessions.

Security Functionality Verification: AMI system shall verify that all security functions within the component are in an online/active state upon component and system startup and restart; upon command by a user with appropriate privilege or periodically.

Separation of Duties and Least Privilege: The utility shall establish appropriate assignment of responsibility and separate duties as needed to eliminate conflicts of interest in the roles. Input to an AMI system that may alter its physical configuration must be limited to personnel who routinely need to make such adjustments in the performance of their duties.
All AMI components shall employ the concept of least privilege for all accounts, protocols, and services and enforce the most restrictive set of roles. Services and protocols shall not be run under root or administrator accounts.

Monitoring, Logging, Reporting: AMI system shall detect, log and report necessary security events, security malbehaviours and system activities to the AMI management system. The utility shall also develop, disseminate, and periodically review and update system and information security policy and procedures.

4. SECURITY SOLUTIONS

4.1. System Constraints

Cost effectiveness (Computation and memory constraints): Smart meters need to be very cost effective because millions will be purchased. The meter needs to perform a number of tasks essentially unrelated to security, such as storing meter readings, interfacing to many different AMI network technologies,, providing self diagnostics, etc. Adding additional features to improve security or adding compute power for encryption/decryption, can increase the cost of the meter [1], [3].

Location: Smart meters will generally be located in very physically unprotected locations since they can easily be reached by the public. Therefore both physical and cyber access could be easily performed [1], [3].

Bandwidth limitation: The smart grid's communications network is mostly composed by low bandwidth (Ziggbee, Wi-fi, narrowband PLC) carriers. So security solutions which needs the transmission of large encryption keys and certificates will be limited by throughput availability [2].

Variety of Network Modules: The entities in smart grid AMI system are a blend of devices from numerous commercial and network providers each having its unique features, communication mechanisms and limitations. Therefore, the security technology emphasizes a complete range of solutions that complies with differing needs of respective network

domains [3]. Additionally, it requires a lot of efforts to model a standardized security framework that accompanies with agreements across different vendors and legacy systems.

Power: Smart meters are battery powered devices so that they still perform metering functions even on loss of power. A cyber-attacks may be accomplished to harvest battery that cause denial of service and unavailability of the meter.

4.2. Security Solutions

Since AMI is a new concept for power distribution solutions, in the literature, there are a few security solutions regarding AMI. In this section these solutions will be given and discussed.

In [4], they proposed a protocol, to provide efficient secure AMI communications by a protocol called integrated authentication and confidentiality (IAC). They claimed that by IAC, an AMI system can provide trust services, data privacy, and integrity by mutual authentications whenever a new smart meter initiates and joins the smart grid AMI network. The proposed IAC protocol employs mutual authentication between a remote server located in the local management office and a neighboring smart meter as the authenticator to obtain proper cryptographic keys for consequent secure data communications. Therefore, readings from smart meters and/or local management offices can employ encryption and message authentication mechanisms tailored for the security requirements and system constraints. In each smart meter and the collecting node, they use a block cipher SEED for encryption/decryption and hash based message authentication code (HMAC) for message authentication code generation.

In [10], they proposed a key management scheme for AMI. The proposed key management framework is constructed based on the key graph. Furthermore, three different key management processes are designed to deal with the hybrid transmission modes, including key management for unicast, broadcast, and multicast modes. They claimed that relatively simple cryptographic algorithms are chosen for key generation and refreshing policies due to the storage and computation constraints of SMs. They used symmetric algorithms (AES-128, HMAC) and hash functions for proposed key management framework.

In [11], they proposed a security architecture for AMI which use Power Line Communication technology. This proposed protocol includes key generation and provisioning to devices without exposure; initialization to authenticate devices in the network and key sharing between devices before exchanging data, secure transmission of meter-reading data, and revocation management to handle discarded devices from the network. They claimed that proposed protocol provides strong authentication of devices and data, prevents a single point of failure by adopting secret sharing through multiple certificate authorities and reduces the risk of denial-of-service attacks on the server by hop-by-hop authentication for data transmitted from terminal nodes to the server. They use a block cipher algorithm for meter readings transmission and the process of deducing a session key from the shared key. The proposed protocol uses an authenticated encryption scheme for encrypting the meter readings and public-key encryption scheme for the encryption of the shared key in the shared key transportation protocol. Also every sub-protocol in proposed architecture exploits the digital signature scheme.

In [12], they claimed that they propose an ID-based authentication protocol for the advanced metering infrastructure, which provides source authentication, data integrity and non-repudiation services, while preserving the end-customer's privacy. Proposed protocol involves three phases: System setup phase, Node initialization/Private key generation phase and Data Source Authentication phase. For signature generation/verification over the certificates, they use the ECDSA signature scheme.

5. CONCLUSION

As a critical component of the smart grid communication infrastructure, AMI is open to variety of security threats for all AMI components including the reliability of smart grid operations due to devices being placed in physically insecure locations. Therefore the holistic design of AMI security architecture is a crucial task.

Since designing security architecture is inevitable for AMI, in this paper, security issues regarding AMI technology is discussed by picturing the possible AMI architecture. AMI security threats and security requirements is given and possible security solutions are discussed by considering system constraints.

6. REFERENCES

[1] F.M. Cleveland, "Cyber security issues for advanced metering infrastructure", *Proc. IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy*, July 2008, pp. 1 – 5

[2] S. Kaplantzis and Y. A. Sekercioglu " Security and smart metering", *18th European Wireless Conference, April 2012*

[3] Mehra, T. and Pateriya, R.K., "Cyber Security Considerations for Advanced Metering Infrastructure in Smart Grid", *Int. J. Sci. Engg. Res. 4(8)*, pp. 939-944, 2013.

[4] Yan,Y., Hu, R., Das, S.,Sharif H., Qian Y., "An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid", IEEE Network, July/August 2013.

[5] Gungor, C., et.al. "A Survey on Smart Grid Potential Applications and Communication Requirements", *IEEE*, 2012.

[6] Advanced Metering Infrastructure Attack Methology, inguardians.com/pubs/AMI_Attack_Methodology.pdf. Lastvisited: 28.03.2014.

[7] Security Profile for Advanced Metering Infrastructure, http://osgug.ucaiug.org/utilisec/amisec/default.aspx. Last visited: 04.01.2014

[8] Choi, Moon-Suk, et al. "A guide to Design of Security Protocol for Advanced Metering Infrastructure."

[9] Y. Ye, Q. Yi, and S. Hamid, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid," in *Proc.*

IEEE WCNC, Cancun, Mexico, Mar. 28–31, 2011,pp. 909–914.

[10] Liu, Nian, et al. "A key management scheme for secure communications of advanced metering infrastructure in smart grid." *Industrial Electronics, IEEE Transactions on* 60.10 (2013): 4746-4756.

[11] Kim, Sungwook, et al. "A secure smart-metering protocol over power-line communication." *Power Delivery, IEEE Transactions on* 26.4 (2011): 2370-2379.

[12] Bekara C., Luckenbach T., and Bekara K., "A privacy preserving and secure authentication protocol for the advanced metering infrastructure with non-repudiation service." *ENERGY 2012, The Second International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies*. 2012.

[13] McLaughlin, Stephen, Dmitry Podkuiko, and Patrick McDaniel. "Energy theft in the advanced metering infrastructure." *Critical Information Infrastructures Security*. Springer Berlin Heidelberg, 2010. 176-187.

[14] HomePlug, http://en.wikipedia.org/wiki/HomePlug, Last visited:04.04.2014.

[15] Adak K., et al. "Advanced Metering Infrastructure Security",http://morse.colorado.edu/~tlen5710/10F/10f _AMISecurity.pdf, Last visited: 04.04.2014.

[16] Costache, Mihai, and Valentin Tudor. "Security Aspects in the Advanced Metering Infrastructure.", *Master of Science Thesis, Chalmers University of Technology University of Gothenburg,* 2011.

[17] AMI System Security Requirements, v1.01, 17.12.2008, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-AMI_System_Security_Requirements_updated.pdf Last visited:01.04.2014

[18] Communications Requirements Of Smart Grid Technologies, http://energy.gov/gc/downloads/communications-requirements-smart-grid-technologies Last visited 01.04.2014

[19] Wikipedia.org, Buffer overflow, Last visited 01.04.2014