Middle-East Journal of Scientific Research 24 (7): 2266-2274, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.07.23204

# Integrated Smart Meter Using Relaible Energy Management Scheme (REMS) for Smart Grid Applications

*[1]K. Vedavalli and [2]N. Muruganantham*

[1]Periyar Maniammai University, Vallam, Thanjavur 613 403, India
[2]Associate Professor and Head / EEE Periyar Maniammai University,
Vallam, Thanjavur 613 403, India

**Abstract:** In the future, energy would cost more as the direct result of steady increases in power generation cost and since the energy consumption may exceed its productions. The idea of designing the integrated wireless energy Meter is due to the basis that it would indirectly helps to create a better understanding and awareness towards the value and the importance of electrical energy, energy saving, promoting of smart energy management as well as an innovation towards further improvement to proven existing system. This paper is mainly focus on consumer awareness on power consumption using integrated wireless communication based Smart energy meter which is basically concentration on our Tamilnadu power scarcity. By realizing such idea, end users are provided with the proposed system to assist them in carefully planning and managing their electrical consumption. Thus, power wastage could also be reduced to the minimum level and helps to ease the arising problems. The smart energy meter, sensor units and Effective communication protocol are integrated to the existing prototype that is capable of sending the energy consumption details in a specified period of time to the electric board. Wireless communication offers the benefits of low cost, rapid deployment, shared communication medium and mobility; at the same time, it causes many security and privacy challenges. The receiver terminal will then display the electrical consumption pricing in a display panel. Microsoft Visual basic C. NET is used as the development platform specifically for the data processing and user interface design. The prototype was meant to compensate the current system and able to provide accurate, reliable and instantaneous meter reading and displays the users' electrical consumption in terms of price unit.

**Key words:** Communication infrastructures · Consumption pricing · Operation transparency · Home area networks

## INTRODUCTION

Power or energy crisis has always be a major critical agenda to the world today. The never ending thirst for energy in industrial, commercial and everyday uses can undoubtedly be solved or at least be made less serious by practicing good power management. The currently assembled kilowatt-hour meter by electrical energy providers will only shows the current electrical consumption in terms of kWh rather than showing the cost of energy that we have spent. Psychologically, the conventional system would not affect the trend of electrical consumption, but when the meter displays the pricing information then it might function accordingly. Real-time pricing gives a real cost-controlling opportunity for those who know the detail load characteristics.

Figure 1 illustrates a general architecture for smart grid communication infrastructures, which includes home area networks (HANs), Industrial area networks (IANs) and neighborhood area networks (NANs), data centers and substation automation integration systems [1]. Smart grids distribute electricity between generators (both traditional power generation and distributed generation sources) and end users (industrial, commercial, residential consumers) using bi-directional information flow to control intelligent appliances at consumers side saving energy consumption and reducing the consequent expense, meanwhile increasing system reliability and operation transparency. With a communication infrastructure, the smart metering/monitoring techniques can provide the realtime energy consumption as a feedback and correspond to the demand to/from utilities.

**Corresponding Author:** K. Vedavalli, Periyar Maniammai University, Vallam, Thanjavur 613 403, India.

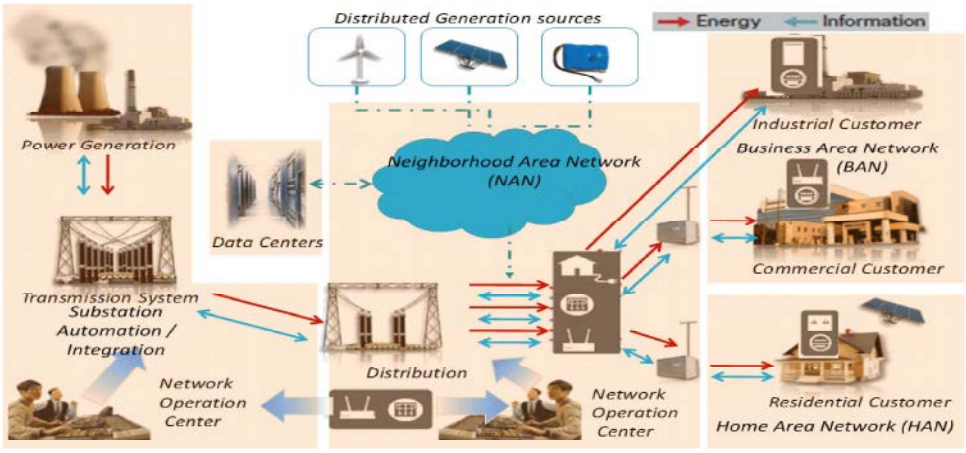


Fig. 1: Smart Grid Communication Infrastructures [1]

Network operation center can retrieve those customer power usage data and the on-line market pricing from data centers to optimize the electricity generation, distribution according to the energy consumption.

Essentially there are two types of electricity meters that were used by the power companies which are the electromechanical and the electronic meter. The display can take in many forms for example cyclotype, digital and the dial type registers. Even though these kilowatt-hour meters are proven to be highly accurate and reliable instrument used to measure electrical energy consumed by the user during the month, it would not shows the latest pricing as well as recording the monthly energy consumption history. The idea is to develop a wireless based energy meter for electrical pricing system which composed of the following elements:-

- An interval meter capable of register energy consumption in a specified period of time.
- A integratedzigbee based communication system that upload usage data and cost details from the meter to a central computer for data processing.
- A display panel on the computer which display the real time pricing and status of the current and previous month details to the user.

The computer then displays the electrical consumption pricing on a display panel. The project is implemented using a standard visual programming language such as the Visual C++. NET for data processing and user interface design. The system also provide with a simple, practical, logically organized and well labeled user interface design. The user interface is designed in such a way so that it would be more users friendly while still maintaining its practicality and workability.

In this work, effective wireless communication technologies are applied to meet the specific requirements for power system generation, transmission, distribution and consumption. Since it is designed as a low cost, low rate, low power and low complexity personal area network, Zigbee is considered as an ideal protocol for smart grid applications, such as real-time system monitoring, load control and building management. The proposed technology is the necessary part of smart grid communication for distribution grids that connect directly to customers because: 1) in home area network, it is too expensive to build wired networks to monitor various devices with different interfaces; 2) when hundreds of parameters in the grid need to be monitored, wired network can result in a costly and complicated system architecture.

**Previous Research:** The authors briefly discuss the latest developments in domestic electricity metering and then discuss meter communications systems for local, remote and automatic meter reading [2]. They describe optical links, pilot wire systems, power line carrier methods, telephones and radio. The suitability and advantages of each type of system is discussed.

A networked remote meter-reading system based on Bluetooth wireless communication technology and GSM is presented in this paper. The remote meter-reading system employs distributed structure, which consists of measure meters, sensors, intelligent terminals, management centre and wireless communication network. The intelligent terminal which designed based on embedded system and Bluetooth technology is used to realize acquisition information submitted from meters and sensors control the energy-consuming devices moreover in residence. The message communicated between the

intelligent terminal and management centre by dint of GSM network. The structure and function of this meter-reading system are described and the system's hardware and software detailed [3]. The meter-reading task can be finished at the management centre of residence area by using this system. The system has many significant excellences, such as wireless, low-workload, great quantity of data transmission, high-veracity and low-expenses. The using of embedded system improves the stability of wireless data transmission. The remote meter-reading system which can be propitious to administer energy-source and continuous development have abroad application foreground.

Recently the Electrical supply companies are trying to adopt the electronic measurement of energy consumption data because of reduced manufacturing cost, improved measurement accuracy, increased timely information, miniature size and many other benefits that go well beyond the traditional rotor-plate energy meter type. In this paper with the help of an energy chip, an improved energy metering solution is developed, where automating the progression of measurement through digital wireless communication technique is adopted to get the above benefits along with smooth control. The developed energy meter calculates the total average active power mainly for residential consumers. The hardware circuit accepts single phase voltage and currents as its inputs and provides the output in the form of logic data proportional to the average real power. This data is fed to a remote computer server through the wireless ZigBee network that represents the concept of distant wireless metering, practically involving no manpower. This paper also presents a software solution developed for total electrical energy billing and data management system [4].

This paper addresses the potential applications of multi-protocol routing for automatic remote meter reading (ARMR). The paper concentrates on the special needs for these applications over the lower line, in terms of: the data on a lower line medium; transmitting and receiving data from any point on the low voltage distribution network; achieving reliable communications from any point on the low voltage distribution network to any other internal and external point; and the ability to increase system performance. Other communications media such as radio and telephone line are not ignored. The intention is to seek out a protocol or multiprotocol routing architecture, which could be used for power line carrier systems but equally could also he applied to these other media for the communication of metering data and other services [5].

There has been increased interest in the ZigBee standard, in particular for building automation and industrial controls. The ZigBee Alliance has identified six application spaces for ZigBee: consumer electronics, PC and peripherals, residential/light commercial control, industrial control, building automation and personal healthcare. This article deals mainly with industrial control and building automation. Increasingly, companies developing monitoring and control applications in industrial and commercial building environments are looking to wireless technologies like ZigBee to save the cost of wiring and installation and also to allow more flexible deployment of systems [6].

Local positioning systems are able to track physical assets or people. Such systems can help, but are not limited to, factory automation, asset management. However, it is not easy to apply such systems at the factory level because they are limited by the challenging environment (e.g., obstacles and hostile environment). Advanced wireless technologies provide a chance to make such applications possible. One of the possible technologies is the ZigBee technology, whereas a brief review of the technology and specification of which is presented in this paper. Since the wireless local positioning systems could be represented as a sensor network, multi-agent system would be a good candidate to model such systems. In this connection, an agent-based wireless local positioning system with ZigBee technology is proposed in this paper. Based on this system, some applications are suggested.

**Security Issues in the Smart Home and the Smart GRID:** Having just exposed some of the most vital benefits arising from the interaction of smart home and smart grid entities, we can now further appreciate the importance of communication amongst the entities of this critical infrastructure. What we should notice however, is that as the connectivity amongst the different entities of the smart grid and/or the smart home increases, the challenges also increase; especially those challenges relative to system security. Thanks to its critical nature, the smart grid can easily become a prime target for terrorists, hackers and vandals aiming to cause anything from a simple discomfort to havoc. Therefore, it is imperative that we start focusing on ways to safeguard its reliable operation and fulfill its security goals.

**Smart Home/Smart Grid Security Objectives:** Clearly describing the security goals the smart home/smart grid environment is expected to meet,

serves as our first step in the effort for ensuring unfailing and consistent smart grid operation. For the purposes of this paper, we consider the six commonly adopted goals described below as the most important for smart home/smart grid security. These goals are:

**Confidentiality:** the assurance that data will be disclosed only to authorized individuals or systems.

**Integrity:** the assurance that the accuracy and consistency of data will be maintained. No unauthorized modifications, destruction or losses of data will go undetected.

**Availability:** the assurance that any network resource (data/bandwidth/equipment) will always be available for any authorized entity. Such resources are also protected against any incident that threatens their availability.

**Authenticity:** the validation that communicating parties are who they claim they are and that messages supposedly sent by them are indeed sent by them.

**Authorization:** the assurance that the access rights of every entity in the system are defined for the purposes of access control.

**Non Repudiation:** the assurance that undeniable proof will exist to verify the truthfulness of any claim of an entity.

**Security Attacks:** Security threats within the smart home/smart grid environment usually attempt to compromise one or more of the security goals we just described. These threats can be classified into two broad categories.

In the first category, namely "passive attacks", we place attacks attempting to learn or make use of information from the system without affecting system resources. In other words, in passive attacks the adversary intends to obtain information being transmitted not to modify it but to learn something from it. Passive attacks can take the form of eavesdropping or traffic analysis. By eavesdropping we refer to the unauthorized interception of an on-going communication without the consent of the communicating parties. By traffic analysis we refer to something subtler. Instead of trying to get hold of message contents, like in an eavesdropping attack, in traffic analysis the adversary monitors traffic patterns in order to deduce useful information from them. Both of these attacks are considered difficult to detect since they do not alter data. Thus, in dealing with them our focus is on prevention rather than detection.

The second category, namely "active attacks", is the category where we place those attacks attempting to alter system resources or affect its operation. Active attacks can involve some modification to data or the introduction of fraudulent data into the system. The most common amongst these attacks are masquerading, replay, message modification, denial of service and malicious software. A masquerading attack takes place when an intruder pretends to be a legitimate entity to gain privileges. A replay attack involves the passive capture of messages in a communication and their retransmission to produce an unauthorized effect. A message modification attack, involves the alteration of the contents of a legitimate message or the delaying or reordering of a stream of messages, aiming to produce an unauthorized effect. A denial of service attack aims to either temporarily or permanently interrupt or suspend the availability of the communication resources of a system.

Finally, malicious software attacks, are attacks aiming to exploit internal vulnerabilities to modify, destroy and steal information or gain unauthorized access to system resources. All the above mentioned threats and many more subcategories of these will be identified for the smart home/smart grid environment in the sections to follow. The security requirements they violate as well as an impact evaluation will also be presented.

**Impact Evaluation:** For the assessment of the criticality and sensitivity of certaininteractions and the evaluation of the impact level of threatsagainst those interactions within the smart home/smart gridenvironment, we adopt FIPS 199, impact level assessmentcriteria [7]. FIPS199 characterizes potential impact of threats as Low, Moderate or High. Where the potential impact is said to be:

- Low (L), if the violation of one or more of the security goals described above can be expected to have a limited adverse effect on smart home's/smart grid's operations, assets or individuals. Limited adverse effect could mean degradation of an entity's capability to efficiently perform its primary functions, minor damage to assets, minor financial losses or minor harm to individuals.
- Moderate (M), if the violation of one or more of the security goals described above can be expected to have a significant adverse effect on smart

home's/smart grid's operations, assets or individuals. Significant adverse effect could mean significant degradation of an entity's capability to efficiently perform its primary functions, significant damage to assets, significant financial losses or significant harm to individuals (not including loss of life or life threatening injuries).

- High (H), if the violation of one or more of the security goals described above can be expected to have a severe or catastrophic adverse effect on smart home's/smart grid's operations, assets or individuals. Severe or catastrophic adverse effect could mean severe degradation or loss of an Entity's capability to perform its primary functions, major damage to assets, major financial losses or severe harm to individuals (that could even result in loss of life or life threatening injuries).

**Smart Home/Smart Grid Security Issues:** Having acquired a more comprehensive view regarding threats to both the smart home and smart grid as individual elements, we can identify some of the main threats that aim at their interaction. This section is dedicated to threats initially affecting or taking control of entities within the smart home that end up affecting entities within the smart grid. The scenarios presented in this section are thus numbered following the symbolic notation SH-SG_number, standing for smart home initiated attacks affecting the smart grid followed by the scenario's serial number. Table 1 provides a more concise view of the threats presented within each scenario of this section, the security goals violated and an impact evaluation.

Table 1: Smart Home to Smart Grid Security Issues

| Scenario num: | Possible Threads | Security Goals Compromised | Degree of Impact |
|---|---|---|---|
| SH_SG1 | ESI Impersonation<br>Message Modification<br>Replay Attacks<br>Jamming Attacks<br>Device Impersonation<br>Repudiation | Integrity<br>Availability<br>Authenticity<br>Non Repudiation | L-M |
| SH_SG2 | Meter Impersonation and Replay attack | Integrity<br>Availability<br>Authenticity | L |
| SH_SG3 | Meter Impersonation / Message Modification<br>Replay attack | Integrity | L-M |
| SH_SG4 | Eavesdropping<br>Message Meditation<br>ManInTheMiddle<br>False Data Injection<br>Denial of Service | Integrity<br>Confidentiality<br>Authenticity | L-H |

**Smart Home/Smart Grid Security Countermeasures:** In this section, we present several promising countermeasures suggested in literature which could be adopted against the different attacks identified in Section III. As tabulated in Tables I-IV, several security goals are compromised. In the following section we see how each of these goals may be fulfilled through a detailed survey of approaches and a comprehensive description of various techniques.

**Ensuring Confidentiality and Privacy:** In thisSection we introduced Confidentiality as the security dimension concerned with preventing unauthorized access to specific information. Confidentiality might not be considered as the most critical dimension of smart grid cyber security; however it is one of the key concerns for the consumers as it is inextricably linked to their privacy. This section is devoted to presenting ways of ensuring confidentiality and privacy within the smart home/smart grid communication environment, as they are proposed in recent literature.

**Ensuring Confidentiality:** The most basic technique of achieving confidentiality nowadays is through cryptography. Modern cryptographic techniques available today, can be classified into two broad categories according to the type of key they use. The first category, includes symmetric key algorithms and it is also known as private-key cryptography, since both sender and receiver share a secret key for their communication. The second category includes asymmetric key algorithms and it is also known as public key cryptography since each of the communicating parties has its public key (known to all other parties) and its private key (which is kept secret) [6,8]. In an effort to ensure greater interoperability amongst security mechanisms within the grid the cyber security Work Group of the National Institute of Standards of the U.S. evaluated (in 2010) the usability and expected lifespan of known symmetric and asymmetric algorithms [9]. Symmetric algorithms (such as the standards AES and TDES) are expected to be used for the purpose of data encryption within the smart grid. Asymmetric algorithms on the other hand, (such as the approved RSA, DSA, ECDSA etc.) are expected to be used for the purpose of digitally signing messages. Of course cryptography is not only used for the purposes of ensuring confidentiality. Many works presented below, regarding ways of providing integrity, authenticity, non-repudiation and even authorization, exploit cryptography in one way or another.

**Ensuring Privacy:** Since their appearance, smart metering deployments have raised numerous concerns for being potentially privacy invasive. As we discuss in the previous section, the consumption data collected by smart meters can reveal a lot about the behavior, activities and habits of the residents within a premise, thus causing fear to customers. To date, various models have been proposed for ensuring the privacy of metering data within the smart home/smart grid environment. Our literature review regarding privacy enhancing technologies has revealed a variety of techniques that can be used alone or in combination to ensure privacy. Some of these techniques are briefly introduced below. Ensuring privacy can be achieved through:

**Anonymization:** A process that removes the link between data and its origin in such a way, that the utility can receive the data it requires for carrying out its computations, but cannot attribute the received data to a specific meter.

**Trusted Aggregators:** The meter or a third trusted party are considered to be trusted entities that can handle the aggregation of metering data and their forwarding to the utility. The utility in such a case can use only the aggregates of data without being able to have access to individual consumption information of participating meters.

**Homomorphic Encryption:** A form of encryption that allows specific types of computations to be carried out on ciphertext and obtain an encrypted result which decrypted matches the result of operations performed on the plaintext. The utility in such a case can decrypt the ciphertext of the aggregate of metering data but not the individual metering of the plaintext.

**Perturbation Models:** Models that introduce random noise from a known distribution to the privacy sensitive metering data, before they are transmitted to utility. The utility receiving the perturbed data reconstructs an approximation of the original data. A tradeoff between the level of privacy achieved and the loss of information exists.

**Verifiable Computation Models:** Models in which the aggregator provides a proof along with the aggregate of metering data, that the calculation has been performed as claimed. Such proof can be provided through a zero knowledge proof system, with the smart meter being the prover and the utility the verifier. In zero knowledge proof the verifier only confirms the prover has the knowledge he claims to have and nothing more than that.

**Data Obfuscation Techniques:** Battery-based approaches that aim to conceal the amount of energy consumed by a premise by buffering or releasing their energy load.

**Ensuring Integrity, Authenticity and Non Repudiation:** Just as important as ensuring the confidentiality of personal data within the smart grid/smart home is to ensure data integrity and authenticity (regardless of their degree of privacy). This section is dedicated to presenting techniques of achieving these two key goals by reviewing related literature.

**Ensuring Integrity:** Inspired by traditional ways of ensuring integrity, cryptographic hashing techniques, designed for high integrity assurance in traditional networks could potentially be applied to the smart grid as well, provided they do not introduce prohibitive delays. When using such techniques the sending side uses a hash function to compute the checksum of the message to be sent and attach it to the original message [10]. Upon receiving the message, the receiving side applies the same hash function to the message and compares resulting hash to the hash attached in the original message. Should the two hashes match, integrity is verified (i.e., it is proven that the message contents have not been altered in transit as a result of e.g., a message modification attack).

Attacks against integrity though are not only confined to message modifications. False data injection attacks, replay attacks, device impersonation attacks and sparse attacks are also considered to be major threats against a system's integrity. Recent literature focusing on these attacks and their countermeasures may be limited; however it doesn't lack interesting ideas. Bhattarai *et al.* in, present their own light weight digital watermarking technique as a simple, low-cost and efficient way to ensure defense against false data injection attacks. Digital watermarking is a technique of embedding digital data inside real time meter readings, with the watermark carrying unique information about the owner of the reading. The purpose ofthe watermark is to validate the integrity of data. Watermarkeddata, are sent from the meter to the utility through high speedunsecured networks that are prone to false data injection attacks. To ensure the successful detection of these attacks, themeters use low rate and secured channels to securely

transmitthe watermarks. The utility thus receives both the watermarksand the watermarked data, in order to correlate them and detectfalse data injection attacks.

**Ensuring Authenticity and Non Repudiation:** Ensuringauthenticity and assuring that we can prove the truthfulness ofany allegation regarding transactions within the smart grid, arealso important for the overall smart grid security.

As we already mentioned above, cryptographic hash functions,are nowadays used for ensuring message integrity againstdeliberate alterations, the same way as checksums are used for detecting inadvertent ones. Similar to cryptographic hashfunctions, with the exception that they make use of a secretkey, are message authentication codes such as HMAC which are amongst the most widely used approaches for achievingauthenticity today [11]. Such schemes can also be used withinthe smart grid and so can digital signature schemes that ensuremessage authenticity via asymmetric encryption. Theseschemes operate on the premise that every communicatingentity has its own public-private key pair. Before sending amessage encrypted with the receiver's public key, the sendercan hash the message and sign the hash with his private key.Upon receiving the message, the receiver uses his private keyto decrypt it and evaluate its hash and the public key of thesender to decrypt the original hash [10]. The two hashes arethen compared, if they match the integrity of the message isproven and so is its authenticity (since no one, other than thesender, could have signed the message with the sender's privatekey). Meanwhile, non-repudiation can also be achieved if thesender demands a signed acknowledgement from the receiver,verifying he indeed received the message.Alternative ways for achieving message authenticity andnon-repudiation specifically designed for the smart grid havealso been proposed in recent literature. Below, we present anumber of interesting approaches.

Nabeel *et al.* in, propose the use of Physically UnclonableFunction (PUF) modules within meters for achievingstrong hardware based authentication of smart metersand efficient key management. Key management guaranteesthe confidentiality and integrity of messages transmitted fromsmart meters to the utility and vice versa. PUFs are functionsembodied in a physical structure inexpensive to manufacturebut impossible to replicate even given the exact manufacturing process. Due to their unclonability they can be described asthe hardware analogs of one-way functions. PUFs implement challenge-response authentication, i.e., they receive a stimulus(challenge) that interacts with their physical microstructure(which is considered to be unique due to the intrinsic randomnessin the fabrication process of integrated circuits) andreact by providing an unpredictable yet repeatable response.PUFs map challenges to responses in a way that cannot bepredicted or replicated. Their properties are exploited by theauthors along with Pedersen commitment scheme and the Zero-Knowledge proof of knowledge protocol to ensure confidentiality,integrity and authenticity but also protect the secret keysused by Smart Meters.

**Ensuring Availability:** Usually, when presenting security requirements for a systemusing the basic CIA triad (Confidentiality, Integrity, Availability)the ordering does not have any specific meaning. However,when it comes to the smart grid/smart home, some stakeholderssuggest that the triad should be prioritized as AvailabilityIntegrity Confidentiality (AIC) so that the ordering reflects thatavailability is the most important goal, followed by integrityand then confidentiality [12].

Aravinthan *et al.* in [13] suggest that the best way todefend against intentional jamming is to use multiple alternatefrequency channels when interference is detected in thecurrent channel. According to them, the AMI and all nodeswithin it, could be programmed to move though a common,predefined sequence of channels, hardcoded into them, if thedefault channel suffers from packet losses that are above anacceptable threshold, for a specified period. Every node thatgets introduced into the AMI network and authenticated to it, receives this predefined channel-hopping sequence encryptedwith the customer's public key. The node then retrieves the sequence by decrypting with the customer's private key andbegins communicating in the current channel used. Accordingto the authors, due to the pseudo randomness of the channel hopping sequence it is considered difficult for the jammer topredict what channel is to be used next and thus to perform ajamming attack against it.

**Ensuring Authorization:** The last security goal we focus on, is authorization, i.e.,the attestation that no entity within the smart home/smart gridenvironment can have access to information or services beyond its authority [14]. Despite, its importance for smart home/smartgrid security the literature on authorization is still limited.Nevertheless, some interesting works have been proposed.

To begin with, we introduce the work of Ruj *et al.* in [14].Their work is based on an architecture consisted of HAN, BANand NAN gateways in one side and RTUs on the other. Eachof the HAN, BAN and NAN gateways in that architecture isresponsible to create an aggregate of its received data, encryptthat aggregate using the Paillier encryption scheme and forwardit further (HAN to BAN, BAN to NAN and NAN to RTU).

Access control in Ruj *et al.* scheme is introduced with the useof an attribute-based encryption variant specifically modifiedby the authors, according to the needs of the smart grid. Intheir paradigm, the RTU collecting data from different units,encrypts those data under a set of attributes before sending themto the data repository they should be kept in. These attributescould be any information related to that data like the sourceof energy (e.g., solar, wind, fossil fuel), the type of consumer (e.g., individual, company, vehicle), the type of equipment (e.g.,dryer, heater), the time of use (e.g., peak, off-peak) etc. In thisway, the RTU creates an access policy for the data it places intothe data repository. Thus, users wanting to have access to themshould first acquire secret keys, corresponding to the attributesof their interest, from a KDC (key distribution center). In thisway, users can only decrypt those data for which they havematching attributes, hence access control is achieved.

**Further Challenges and Future Directions:** Thus far, we have identified illustrative scenarios of interactionamongst entities of the smart home and the smart grid.We have analyzed potential cyber and physical security threats,

- Establishing a universal standardization framework forsecure communication within the smart home and thesmart grid.
- Establishing authorities to evaluate the conformance ofsmart home/smart grid industry to the different voluntarystandards.
- Establishing new/altering old protocols with respect to thesmart grids unique requirements.
- Establishing new metrics for the evaluation of the cybersecurity mechanisms and solutions suggested.
- Evaluating the security implications arising from the introductionof PHEVs/PEVs and Distributed Energy Resourcesas part of the smart grid and the smart home.
- Establishing a legal framework specific to smart gridprivacy.
- Establishing new aggregation schemes that do not involvea trusted aggregator.
- Establishing new techniques for facing jamming attacks.
- Establishing Intrusion Detection, Intrusion Prevention andIntrusion Recovery Systems specifically for the smart grid.
- Designing systems that can support the logging of informationfor the purposes of audit controls and forensicsanalysis.
- Establish more key management techniques specificallyfor the AMI and the Wide Area Measurements Network.

Critical messages are also exchanged within another type ofnetwork in the smart grid, the Wide Area Measurement Network.Such a network consists of many sub-networks equippedwith advanced metering technology (such as PMUs). Their purposeis to enhance the operator's real-time situational awareness through regular reports of the grid's current state. The measurements collected from different phasor-measurement sitesreveal abnormalities and trigger immediate action to protect thegrid's equipment in cases of emergency thus maintaining theirintegrity is of primary importance for the overall functioning ofthe grid.

Despite the significance of these messages however, to date,the majority of key management schemes proposed for securingcommunications within the smart grid, address the establishmentof keys for the communicating entities within the SCADAsystems only. In fact, few research studies have been carriedout on key management schemes for the AMI entities and theWide Area Measurement Network entities. For this reason, webelieve additional research should be focused on the creation ofkey establishment schemes specifically designed for the AMIand the Wide Area Measurement Networks.

## CONCLUSION

In this paper we presented dangers looming under some ofthe most illustrative scenarios of interaction amongst entitiesof the smart home/smart grid environments, evaluating theirimpact on the entire grid. In addition to that, we conducteda review of recent literature on potential solutions and countermeasures, aiming to identify approaches for prevention ordefense against attacks that could help us achieve the securityobjectives we set for both the smart home and the smart grid.Smart grid cyber security standardization efforts across theglobe were also outlined, whereas a section devoted to openchallenges and future directions

for research served as theconclusion of our paper. Through that section, we suggestedseveral topics that need to be further investigated.The heterogeneity of the smart home/smart grid environmentdoes not leave room for "one-size-fits-all" security solutionsmaking smart home/smart grid security a challenging yetpromising research field for the future.

## REFERENCES


1. U.S. Department of Commerce, National Institute of Standards and Technology, NIST Special Publication 1108, NIST Framework and Roadmapfor Smart Grid Interoperability Standards, Release 1.0, Jan. 2010. [Online]. Available: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.
2. Alam, M.R., M.B.I. Reaz and M.A.M. Ali, 2012. A review of smarthomes-Past, present and future, IEEE Trans. Syst., Man, Cybern., C. Appl. Rev., 42(6): 1190-1203.
3. Wang, W. and Z. Lu, 2013. Cyber security in the smart grid: Survey and challenges, Comput. Netw., 57(5): 1344-1371.
4. Li, X., 2012. Securing smart grid: Cyber attacks, countermeasures and challenges, IEEE Commun. Mag., 50(8): 38-45.
5. Kim, Y.J., M. Thottan, V. Kolesnikov and L. Wonsuck, 2010. A secure decentralized.
6. Data-centric information infrastructure for smart grid, IEEE Commun. Mag., 48(11): 58-65.
7. Mantas, G., D. Lymberopoulos and N. Komninos, 2010. Security in smart home environment, in Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications.
8. ENISA, 2012. Annex I. General Concepts and Dependencies With ICT ofENISA Study Smart Grid Security: Recommendations for Europe andMember States, Jun. 2012. [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/.
9. Lazakidou, A., K. Siassiakos and K. Ioannou, Eds. P.A. Hershey, USA: Medical Information Science, 10: 170-191.
10. Kamilaris, A., A. Pitsillides and M. Yiallouros, 2013. Building energy-aware smart homes using web technologies, J. Ambient Intell. Smart Environ. (JAISE), 5(2): 161-186.
11. Zhang, Y., L. Wang, W. Sun, R.C. Green and M. Alam, 2011. Distributedintrusion detection system in a multi-layer network architecture of smartgrids, IEEE Trans. Smart Grid, 2(4): 796-808.
12. CITIPOWER, Powercor, Load Shedding, 2013. [Online]. Available: http://www.citipower.com.au/Electricity_Networks/Power_Outages_Explained/Load_Shedding/
13. smart-grids-and-smart-metering/ict-inderdependencies-of-the-smart-grid/IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation With the Electric Power System (EPS), End-Use Applications and Loads, IEEE Std. 2030-2011, Sep. 10, 2011, pp: 1-126.
14. BSOL Batteriesysteme GmbH, Smart Grid Solutions. [Online]. Available: http://www.bsol.de/files/Tech Notes/Smart%20Grid%20-%20A3.pdf.