Communication Security for Smart Grid Distribution Networks

Article *in* IEEE Communications Magazine · January 2013

DOI: 10.1109/MCOM.2013.6400437

Elias Bou-Harb
Louisiana State University
163 PUBLICATIONS **3,047** CITATIONS
SEE PROFILE

Claude Fachkha
University of Dubai
41 PUBLICATIONS **686** CITATIONS
SEE PROFILE

Makan Pourzandi
Ericsson
155 PUBLICATIONS **1,739** CITATIONS
SEE PROFILE

Mourad Debbabi
Concordia University Montreal
466 PUBLICATIONS **7,601** CITATIONS
SEE PROFILE

Communication Security for Smart Grid Distribution Networks

Elias Bou-Harb, Claude Fachkha, Makan Pourzandi, Mourad Debbabi, Chadi Assi

***Abstract*—The operation and control of the next generation electrical grids will depend on complex network of computers, software, and communication technologies. Their compromise by a malicious adversary will cause significant damage, including extended power outages and destruction of electrical equipment. Moreover, the implementation of the smart grid will include the deployment of many new enabling technologies such as advanced sensors and metering and the integration of distributed generation resources. Such technologies and various others will require the addition and utilization of multiple communication mechanisms and infrastructures that may suffer from serious cyber vulnerabilities. These need to be addressed in order to increase the security and thus the utmost adoption and success of the smart grid.**

In this paper, we focus on the communication security aspect which deals with the distribution component of the smart grid. Consequently, we target the network security of the advanced metering infrastructure coupled with the data communication towards the transmission infrastructure. We discuss the security and the feasibility aspects of possible communication mechanisms that could be adopted on that subpart of the grid. By accomplishing this, the correlated vulnerabilities in these systems could be remediated and associated risks may be mitigated for the purpose of enhancing the cyber security of the future electric grid.

I. Introduction

The current electrical grid is perhaps the greatest engineering achievement of the 20^{th} century. However, it is increasingly outdated and overburdened, leading to costly blackouts and burnouts. For this and various other reasons, transformation efforts are underway to make the current electrical grid *smarter*.

The smart grid could be referred to as the modernization of the current electric grid for the purpose of enabling bi-directional flows of information and electricity in order to achieve numerous goals; it will provide consumers with diverse choices on how, when, and how much electricity they use. It is self-healing in case of disturbances, such as physical and cyber attacks and natural disasters. Moreover, smart grid's infrastructure will be able to link and utilize a wide array of energy sources including renewable energy producers and mobile energy storages. Additionally, this infrastructure aims at providing better power quality and more efficient delivery of electricity. Indeed, all these goals could not be achieved and realized without a communication technology infrastructure that will gather, assemble and synthesize data provided by smart meters, electrical vehicles, sensors, and computer and information technology systems.

A. Cyber Security Motivation

History has proven that industrial control systems were in fact vulnerable and victims of cyber attacks. In March 2007, Idaho National Laboratory conducted an experiment in which physical damage was caused to a diesel generator through the exploitation of a security flaw in its control system. Additionally, during the Russian-Georgian war in 2008, cyber attacks widely believed to have originated in Russia, brought down the Georgian electric grid during the Russian army's advance through the country. Besides that, in April 2009, the Wall Street Journal reported that cyber spies had penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system. Lastly but very significantly, in 2010, Stuxnet, a large complex piece of malware with many different components and functionalities, targeted Siemens industrial control systems and exploited four zero-day vulnerabilities running Windows operating systems. As a result, 60% of Iranian nuclear infrastructure was targeted and hence triggering a genuine fear over the commence of a cyber warfare.

It is therefore of utmost importance to address the cyber security aspect of the smart grid, specifically the area concerned with the communication mechanisms which deal with the distribution subpart.

The rest of the paper is organized as follows: Section II pinpoints some related work in our concerned area while Section III illustrates and describes the smart grid architecture. Section IV thoroughly elaborates on the feasible communication mechanisms in the distribution part of the smart grid, by revealing their security objectives, security threats, and their practically applicable implementation on the future grid. Section V presents a discussion of the security framework that is needed to enable those communication techniques. Finally, Section VI summarizes and concludes this paper.

II. Related Work

In this section, we briefly highlight some of the work done in the communications and security area in the context of smart grid distribution.

Metke et al. [1] discussed key security technologies for a smart grid system including public key infrastructures (PKI) and trusted computing for various smart grid communication networks. They thoroughly presented the security requirements that are essential for the proper operation of the future grid. In another research work, Yu et al. [2] identified the fundamental challenges in data communications for the smart grid and introduced the ongoing standardization effort in the industry. Moreover, the authors depicted the communication infrastructures, namely, home area networks (HANs) and neighborhood area networks (NANs), and very briefly listed the mechanisms utilized to achieve their architectures. In another paper entitled ‘Secure Communications in the Smart Grid’ [3], the authors focused on HANs by elaborating on its AMI infrastructure, its security issues and requirements. The authors expressed their model in terms of secure communication mechanism on that subpart of the grid.

To the best of our knowledge, the work being presented in this paper is unique by providing significant, relevant, and practical information on the communication mechanisms in both HANs and NANs, by focusing on their security, including their objectives and threats, in additional to their practical feasibility, requirements, and security issues when implemented on the smart grid.

III. Smart Grid Architecture

In this section, we provide a high level overview of the architecture of the smart grid as depicted in Figure 1. The future electric grid has a tiered architecture to supply energy to consumers. Energy starts from power generation and flows through transmission systems to distribution and eventually to consumers. The smart grid is striving to utilize and coordinate various generation and production mechanisms. Moreover, generation plants can be mobile or fixed depending on specific architectures. On the transmission side, a large number of substations and network operating centers manage this task. A large number of mixed voltage power lines transmit the generated electricity from various sources to the distribution architecture. Finally, a set of complex distribution topologies delivers the electricity to regions, neighbors and premises for utilization and consumption.

In this paper, our interest lies in the distribution part of the smart grid. More specifically, we are concerned with the communication networks of that subpart of the grid, namely the Home Area Network (HAN) and the Neighborhood Area Network (NAN). These networks are critical for data communications between the utility and end-users. HANs are composed of three components. First, the smart in-house devices that provide demand-side management such as energy efficiency management and demand response. Second, the smart meter that collects data from smart devices and invokes certain actions depending on the information it retrieves from the grid and thirdly the HAN Gateway which refers to the function that links the HAN with the NAN. This gateway can as well represent the physical device dedicated to performing this functionality. On the other hand, a NAN connects multiple HANs to local access points where transmission lines carry out the data towards the utility.

IV. Communication Mechanisms

In this section, we focus on the communication security aspect that deals with the distribution and the consumption components of the smart grid. In the remainder of this section, we follow the subsequent methodology. First, we **pinpoint the most applicable and utilized communication mechanisms** that could be adopted on that subpart of the grid by introducing their technology and use. Second, we discuss their **security objectives** including confidentiality, integrity, authentication and authorization. Third, we elaborate on their **threats and vulnerabilities**. Finally, we discuss their **feasibility** in context of their implementation and security on smart grid HANs and NANs.

A. HAN Communication Mechanisms

AMI is the key element in smart grid HANs [4]. It is dubbed as the convergence of the power grid, the communication infrastructure and the supporting information architecture. It refers to the systems that measure, collect, and analyze energy usage from advanced smart devices, including, in-home devices as well as electric vehicles charging, through various communication media, for the purpose of forwarding the data to the grid. Thus, this critical communication infrastructure ought to be discussed and investigated.

1) Wireless LAN: The 802.11 is a set of standards developed for wireless local area networks (WLAN). It specifies an interface between a wireless device and a base station (access point) or between two wireless devices (peer-to-peer).

The 802.11 provides confidentiality by implementing the advanced encryption standard (AES). Integrity is achieved through the AES-CBC-MAC algorithm [5] while authentication is implemented using the standards Wi-Fi Protected Access. IEEE 802.11 by default, does not offer authorization mechanisms.

The protocol suffers from significant security threats. It is vulnerable to traffic analysis, a technique which allows the attacker to determine the load on the communication medium by monitoring and analyzing the number and size of packets being transmitted. It is as well susceptible to passive and active eavesdropping where an attacker can listen to the wireless connection as well as actively injecting messages into the communication medium. Moreover, 802.11 is vulnerable to man-in-the-middle, session hijacking and replay attacks.

On one hand, it can be declared that the WLAN (802.11) technology may be a feasible solution in a HAN. As a result, all smart devices should be equipped with an embedded WLAN adapter. Those devices would directly communicate with a WLAN home gateway that could as well be a WLAN enabled smart meter. The authentication mechanism is performed according to a one-to-one basis between the smart device and the gateway. On the other hand, it can be claimed that the 802.11 may not be a suitable communication mechanism for a HAN. This statement can be based on the significant negative consequences that will result if a 802.11-based HAN network was maliciously attacked. For example, suppose the WLAN session is hijacked; then, the attacker

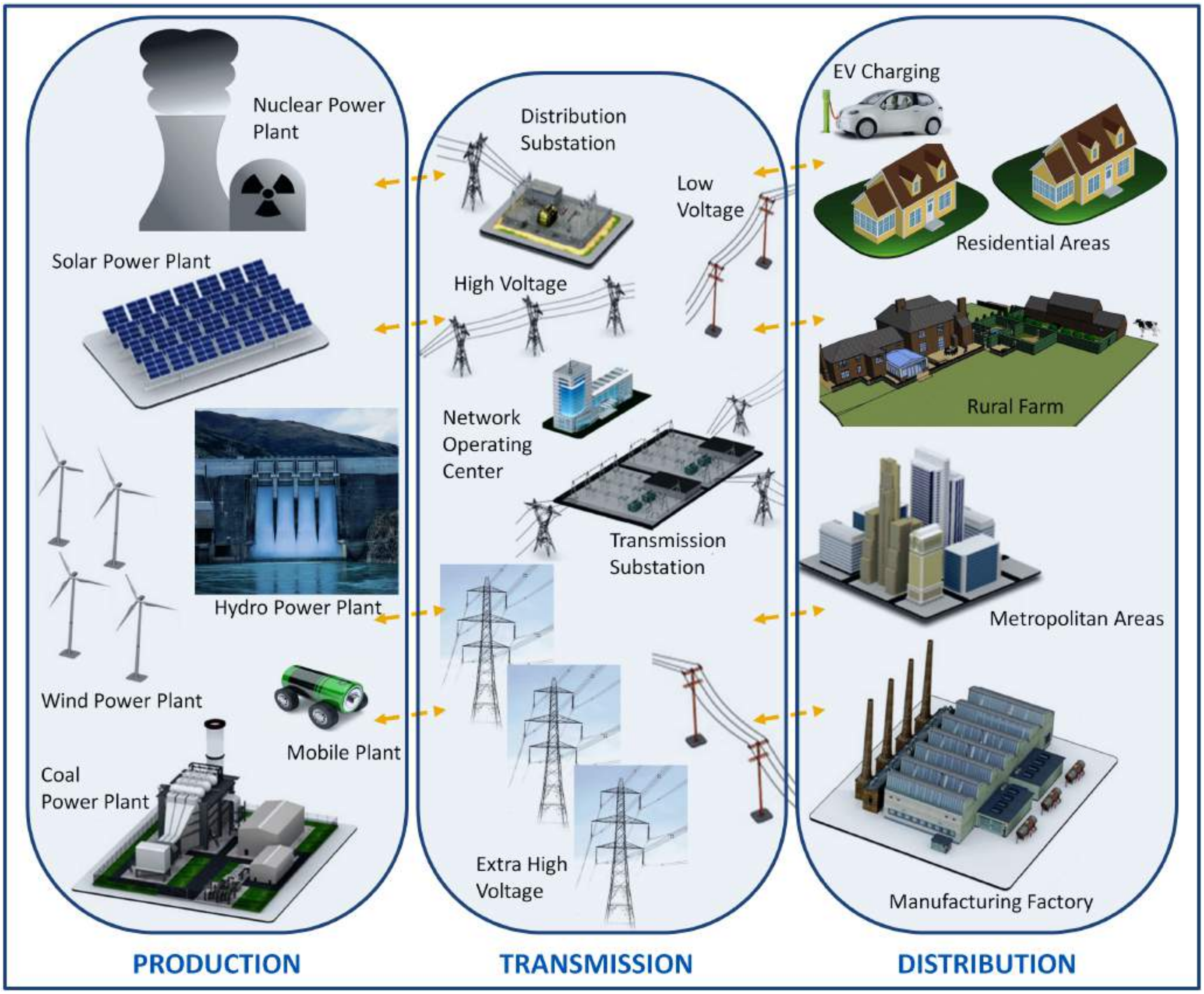

Fig. 1. Smart Grid Architecture

would manipulate the smart devices and corresponding output data and hence forward falsified information to the grid. More simply, assume an attacker was able to jam a WLAN communication by generating random data. Thus, this will cause a serious issue with the availability of the HAN network, causing a DoS that affects not only the functionality of the concerned network, but other dependent smart grid networks as well, including NANs. Furthermore, presume that an attacker was capable of performing traffic analysis on the WLAN traffic in a HAN. Consequently, the confidentiality of the information would be targeted since the attacker would infer HAN consumption loads of various smart devices. In conclusion, we believe that WLAN, with its open standards, high throughput, strong home market penetration, good economics and relatively secure communication, is a suitable choice in a HAN.

2) ZigBee: ZigBee is a specification for a communication protocol using small, low-power digital radios based on the IEEE 802.15.4 standard. It is more specifically known as Low-Rate Wireless Personal Area Networks (LR-WPAN). Confidentiality of a Zigbee network is established though utilizing the AES algorithm. Moreover, frame integrity is achieved by generating integrity codes. ZigBee devices authenticate by employing pre-defined keys. Additionally, ZigBee networks provide security counter-measures against message replays by ensuring freshness of transmitted frames. The 802.15.4 protocol is vulnerable to jamming. This threat aims at weakening the availability of system services. Another threat is characterized by message capturing and tampering, which are difficult to avoid in LR-WPANs, since the cost of sufficient physical protection defeats the low cost important design goal of such networks. A further threat is exhaustion; a compromised coordinator node can lure a large number of nodes to associate with it by appearing to be a coordinator with high link quality. Consequently, it can force all the devices to stay active for most of the time, resulting in quick battery depletions at those devices.

In 2007 a large stakeholder community assembled the ZigBee Alliance to tackle the AMI and develop what is known as the ZigBee Smart Energy. Hence, this extensively advocates the feasibility of adopting the ZigBee technology as a HAN communication infrastructure. As a result, a ZigBee gateway device supporting two communication streams joining the utility AMI central database to smart devices in the HAN need to be placed and configured. The gateway can as well act as a trust center and firewall in the ZigBee network implementation to protect assets from the grid side. To complete the network topology, in-house smart devices equipped with ZigBee modules should be configured and authenticated. However, a core security threat resides if, for instance, an adversary was able to compromise a HAN coordinator ZigBee node. As a result, this node will be able to maliciously control all aspects of other smart device nodes, tamper with their transmitted data, falsely redirect their communications or even deplete their batteries for a complete system failure. Additionally, suppose an attacker was capable of jamming or flooding the ZigBee HAN network. Consequently, this will trigger a drastic availability problem that halts the network which will propagate, negatively affecting all other segments of the grid's communications and functionality. In summary, we believe that ZigBee, with its extremely low cost (e.g. less than $10), low power consumption, unlicensed spectrum use and its already available relatively secure 'smart energy' products, is an extremely effective and efficient communication choice in a HAN.

3) Mobile Communications and Femtocells: Femtocells are cellular network access points that connect in-house user equipments (UEs) to mobile operators' core network infrastructure using residential DSL, cable broadband connections, or optical fibers. The technologies behind femtocells are cellular such as UMTS and LTE. One key driver of femtocells is the demand for higher indoor data rates which can be achieved through the establishing of high performance radio frequency links with a femtocell. Additionally, these devices can significantly provide power savings to indoor UEs since the path loss and the required transmitting power to interface with a femtocell is significantly less than to communicate with an outdoor base station. This fact renders the applicable feasibility of mobile communications and femtocells in HANs.

In a femtocell networking environment, confidentiality and integrity of the transmitted data are guaranteed by using end-to-end IPsec. Moreover, authentication can be realized by using either the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) or the EAP-Subscriber Identity Module (SIM).

In femtocell networks, there are three main security concerns or threats. The first is characterized by network and service availability. Since the link between the femtocell and the core network is IP based, DoS and other flooding attacks are viable. The second is depicted by fraud and service theft where an adversary can connect to a femtocell and make illegal use of it. The third threat targets privacy and confidentiality where the femtocell network is subject to the same security issues of regular IP based networks including fabrication and modification of data.

The adoption of mobile femtocells as a HAN communication mechanism could be a practical, reasonable and a sufficient solution. This is especially true in rural HANs where other communication infrastructures are unavailable but a satisfactory Internet link is accessible. Hence, if this architecture is realizable, then the smart devices including, at least, the smart meter should be equipped with a cellular SIM card. The authentication could be achieved using EAP-SIM [6] between the smart devices and the femtocell. Alternatively, smart in-house devices can authenticate to the smart meter and then the latter can relay the communication to the femtocell. In order to enable access to the femtocell, two access methods could be utilized, namely, closed access and open access [7]. Issues in the deployment of the mobile femtocells technology in HANs could be rendered in three obstacles. First, there is a concern with the use of femtocells in homes with regards to their possible associated health issues [8]. Second, there is the challenge related to the ability of determining femtocells location. This estimation is necessary for smart grid operators to determine HAN locations for network planning and access control reasons which could be hard to achieve using femtocells. Third, there is a security concern by grid operators who will question the transfer of sensitive HAN data through the public Internet as a transmission medium towards the NAN and eventually the grid. In conclusion, we believe that cellular femtocells, with their relatively high price (e.g. > $100), possible indoor health issues, various implementation and security concerns, and limited device access, are not a suitable communication choice in a HAN.

Note that, the distribution part of the smart grid, namely, HANs and NANs with corresponding possible threats, is focused on and illustrated in Figure 2.

B. NAN Communication Mechanisms

Neighborhood Area Network (NAN) is the HAN complementary network that completes the distribution subpart of the smart grid. A NAN is the next immediate tier and its infrastructure is critical since it interrelates and connects multiple HANs collectively for the purpose of accumulating energy consumption information from households (the HANs) in the neighborhood and delivering the data to the utility company. Thus, the communication infrastructure that is responsible for such tasks is as well very significant to confer.

1) WiMAX: The IEEE 802.16 standard, referred to as Worldwide Interoperability for Microwave Access (WiMAX), defines the air interface and medium access control protocol for a wireless metropolitan area network (WMAN).

WiMAX standards define three steps to provide secure

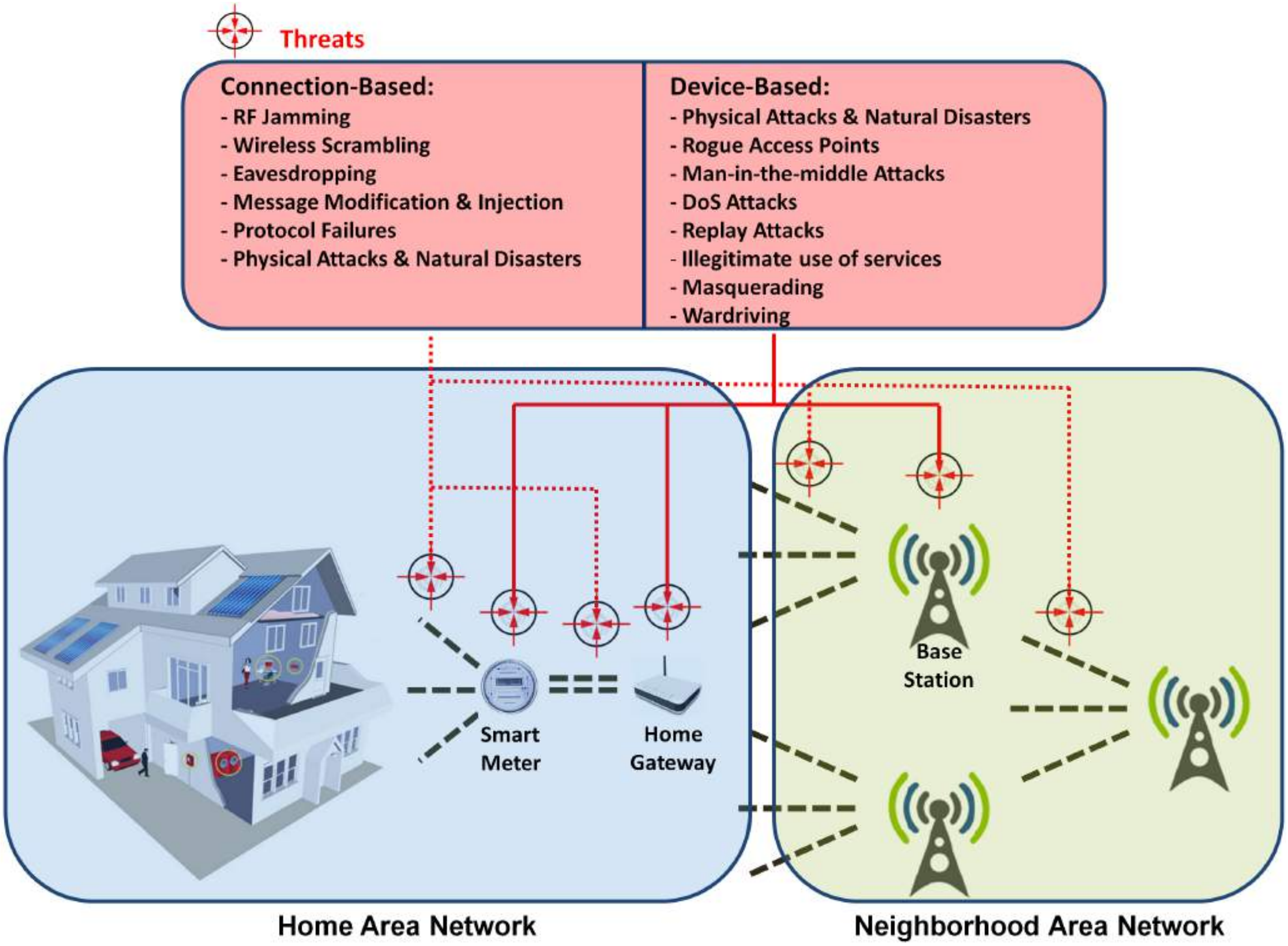

Fig. 2. Smart Grid Distribution and Corresponding Threats

communications, namely, authentication, key establishment, and data encryption. This is achieved by implementing the EAP protocol, the Privacy Key Management protocol and the AES algorithm respectively.
Threats in IEEE 802.16 focus on compromising the radio links. Hence, the system is vulnerable to radio frequency (RF) jamming. WiMAX is as well susceptible to scrambling attacks, where an adversary injects RF interference while transmitting specific management data. This attack affects the proper network ranging and bandwidth sharing capabilities. Additionally, and due to lack of frame freshness, the 802.16 is vulnerable to replay attacks.

The Smart Grid Working Group [9] acts as a major point for utility interests in WiMAX as a technology for smart grid networks. Thus, it promotes WiMAX as a core communication technology for NANs. Furthermore, WiMAX is a broadband wireless last mile technology that can support smart grid distribution. As a result, WiMAX can be implemented between a base station and the home gateway. The smart meter would collect smart devices data and then forwards them to the home gateway which has the interoperability property to comprehend WiMAX communication. The home gateway is in fact a subscriber station (SS) in the HAN. The SS would collect the data from the smart meter and sends it to the NAN through a WiMAX dedicated connection. To complete the data transfer towards the utility, a point-to-point, point-to-multipoint or hybrid (multi-hop relay) [10] WiMAX topologies can be implemented. The practical feasibility of such a technology could be hindered by possible security misdemeanors. For example, and since WiMAX is susceptible to traffic analysis techniques, an adversary with malicious intentions can retrieve HANs sensitive data while in transit through WiMAX to identify neighborhoods trends in consumption loads. Moreover, an attacker can take advantage of lack of message timeliness to launch a man-in-the-middle attack by replaying certain information from the grid or the NAN towards the HANs using WiMAX. In summary, we believe that WiMAX, with its high throughput, significant smart grid standardization and working groups, backhaul media for WiFi or ZigBee in-premises devices, and its interoperability features, is very applicable as a NAN communication technology.

2) LTE: Long Term Evolution (LTE) is a wireless communication standard for a fourth generation mobile network. LTE features an all-IP flat network architecture, an end-to-end quality of service, peak download rates nearing 300 Mbps and upload rates of 75 Mbps. This renders it very advantageous to exist as a NAN communication mechanism.

LTE networks provide mutual authentication between the UE and the core network by implementing the authentication and key agreement (AKA) protocol. For radio signaling, LTE provides integrity, replay protection, and encryption between the UE and the base station (e-NB). Internet Key Exchange (IKE) coupled with IPsec can protect the backhaul signaling between the e-NB and the core network [11]. For user-plane traffic, IKE/IPsec can similarly protect the backhaul from the e-NB to the core network.

Threats in LTE can be divided into three main sections. The first is characterized by attacks on the air interface. Such attacks are mainly passive such as traffic analysis and user tracking. The second is rendered by attacks on the e-NB. Such threats include physical tampering with the e-NB, fraudulent configuration changes, DoS attacks, and cloning of the e-NB authentication token. The third section is characterized by attacks against the core network. These may include flooding and signaling attacks.

In the context of the smart grid, the adoption of LTE as a NAN technology could be feasible in two ways. The first is the use of the already implemented mobile network architecture of established mobile network operators (MNO) to carry out the data. This method can be referred to as piggyback where smart devices data from HANs are piggybacked on the MNO infrastructure as a medium to reach the NAN and eventually the utility. An advantage of this approach is the ease of implementation and adoption since from a smart grid perspective, there is no additional needed configuration, setup and management. The second way in which LTE could be adopted is by utilizing a specialized network core architecture to transfer the data. This methodology itself can be realized in two ways. The first is by implementing the notion of Mobile Virtual Network Operator (MVNO), which means that the smart grid utility rents a portion of the traditional MNO core network for its dedicated functions. The second way is essentially recognized when the utility implements its own core architecture, using the same LTE technologies as the MNO, but totally decoupled from it.

One critical security issue that may thwart LTE as a NAN communication mechanism is the fact that the e-NB is the main location where users' traffic may be compromised [11]. Hence, if various attacks on the e-NB are successful, they could give attackers full control of the e-NB and its signaling to various nodes. In this case, HANs and NANs on the grid and their communications would also be compromised since in such architecture, they play the role of subscribers to the e-NB in the LTE/smart grid infrastructure. To conclude, we believe that LTE, being cost-effective coupled with its relatively rapid implementation and highly secure, available and trustful infrastructure, is a suitable NAN communication mechanism.

Note that, a high level illustration of the discussed communication mechanisms in smart grid distribution networks is shown in Figure 3.

3) Broadband over Power Lines: Advanced signal processing techniques and standardization efforts performed by the European Committee for Electro-technical Standardization have made the employment of narrow band power line communications (PLC) possible. The evolution of this technology gave birth to broadband over power lines (BPL) systems. BPL offers high speed data communications with minimal new infrastructure to deploy making this technology a viable mechanism for NAN communications.

In terms of security objectives, no default security protocols are provided by the PLC MAC standards to achieve access control.

Power line channels are considered to be shared networking mediums and hence external and internal attacks are feasible on such networks. External threats refer to eavesdropping on exchanged data without having access credentials. On the other hand, internal threats are performed by benign users on the network using access credentials with the intent to misuse services.

PLC is a system that could potentially be used in NANs on the smart grid. Many standards such as ITU G.Hn and IEEE P1901 exist. We believe that a harmonized PLC standard is possible by interoperating these systems for a better implementation of the BPL for smart grid. However, a major obstacle for such adoption is rendered by the fact that electric transformers block the transmission frequency of the BPL. This limits BPL to small coverage range within the low voltage grid (neighborhood) and requires other retransmission mechanisms to allow the full data transfer to the utility. From a security perspective, an attacker may be able to launch a man-in-the-middle attack by forging his identity and standing between a HAN and NAN communication using BPL. Moreover, an adversary can take advantage of the use of copper wiring in PLC to sniff the data. In summary, we consider that the BPL technology will unlikely emerge as a leading broadband tool for smart grid NANs, but instead will remain as an option for NAN communication in the future smart grid.

In the subsequent section, we present a discussion on the security framework that is needed to enable the above mentioned communication techniques to be employed for smart grid applications.

V. Security Framework Discussion

Currently, there is a lack of adequate work in security schemes and frameworks for AMI, especially in authentication methods. To the best of our knowledge, there exist very limited realistic approaches [12] to solving the scalability problem of smart meter authentications, regardless which communication technology is utilized.

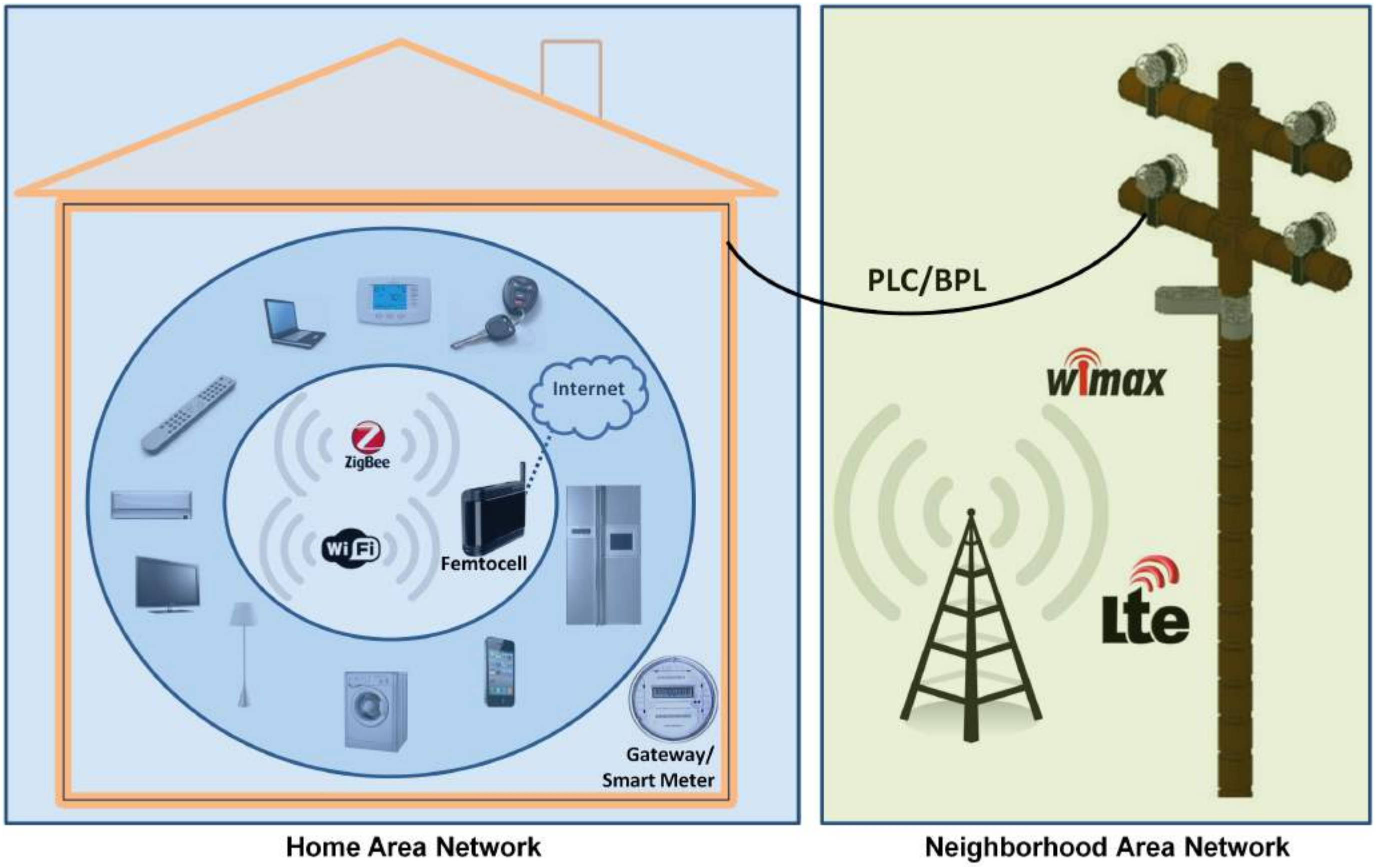

Fig. 3. Distribution Network-Communication Mechanisms

Cryptographic methods such as digital certificates require a momentous overhead in comparison with data packet processing. In addition, cryptographic operations contribute to extensive computational cost. In the context of smart grid, a smart meter routinely sends a meter reading message within a period of 500 ms [13]. Nowadays, for PKI-based schemes, generating a digital signature every 500 ms is not an issue using a commodity computer. Conversely, for a legacy power grid that interconnects numerous buildings, the number of meter reading messages that require verification by the NAN gateway might be particularly larger than its capacity. Although digital signing and message verification can certainly achieve secure communications, however, we believe that the conventional cryptographic operations make such security frameworks neither scalable nor affordable.

We assert that the security framework that is required to enable the discussed communication techniques to be employed for smart grid applications should be based on the following design objectives:

1) Device authentication: The identity and legality of the smart meters and their associated consumers should be verified receiving the proper utility services.
2) Data confidentiality: The smart meter readings and management control messages should be confidential to conceal both consumers' and utilities' privacy.
3) Message integrity: The smart grid should be able to verify that any meter messages should be delivered unaltered in an AMI.
4) Prevent potential cyber attacks: Smart meters should be guaranteed to obtain secure communication with the AMI network, even if an individual smart meter is compromised.
5) Facilitating communication overhead: The proposed framework should be efficient in terms of communication overhead and processing latency.

VI. Conclusion

In this paper, we have investigated applicable communication mechanisms that could be adopted on smart grid distribution networks. To tackle the cyber security of such infrastructures, we have pinpointed their security objectives and threats. We further elaborated on their practical feasibility in terms of their technical implementation, possible obstacles, and their core security issues and attacks on smart grid HANs and NANs.

We believe it is critical to continue discussing, designing, and implementing solutions for such mechanisms for the purpose of enhancing the cyber security of the future electric grid and hence accomplishing consumers' utmost trust in such a major gird transformation.

References

[1] A.R. Metke and R.L. Ekl. Security technology for smart grid networks. *Smart Grid, IEEE Transactions on*, 1(1):99 –107, june 2010.

[2] Rong Yu, Yan Zhang, S. Gjessing, Chau Yuen, Shengli Xie, and M. Guizani. Cognitive radio based hierarchical communications infrastructure for smart grid. *Network, IEEE*, 25(5):6 –14, september-october 2011.

[3] J. Naruchitparames, M.H. Gunes, and C.Y. Evrenosoglu. Secure communications in the smart grid. In *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, pages 1171 –1175, jan. 2011.

[4] U.S. Department of Energy. AMI System Security Requirements, 2008. Available at: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-AMI_System_Security_Requirements_updated.pdf.

[5] Arunesh Mishra, Nick L. Petroni, William A. Arbaugh, and Timothy Fraser. Security issues in ieee 802.11 wireless local area networks: a survey. *Wireless Communications and Mobile Computing*, 4(8):821–833, 2004.

[6] H. Haverinen, Ed. & J. Salowey, Ed. Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)), 2006. Available at: http://merlot.tools.ietf.org/html/rfc4186.

[7] V. Chandrasekhar, J. Andrews, and A. Gatherer. Femtocell networks: a survey. *Communications Magazine, IEEE*, 46(9):59 –67, september 2008.

[8] J. Zhang and G. de la Roche. *Front Matter*, pages i–xxix. John Wiley & Sons, Ltd, 2009.

[9] The WiMAX Forum. Technical Activities and Working Groups), 2011. Available at: http://www.wimaxforum.org/about/technical-activities-and-working-groups.

[10] National Institute of Standards and Technology. Guide to Securing WiMAX Wireless Communications: Recommendations of the National Institute of Standards and Technology, 2010. Available at: http://csrc.nist.gov/publications/nistpubs/800-127/sp800-127.pdf.

[11] Rolf Blom, Karl Norrman, mats Nslund, stefan Rommer and Bengt sahlin. Security in the Evolved Packet System, 2011.

[12] Ye Yan, Yi 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*, pages 909 –914, march 2011.

[13] Ruby Elena Castellanos and Paulo Millan. Design of a wireless communications network for advanced metering infrastructure in a utility in colombia. In *Communications Conference (COLCOM), 2012 IEEE Colombian*, pages 1 –6, may 2012.