Short Communication

Open Access

Security issues in AMI network

Abstract

Smart Grid is now the need of homes, utilities, and the customers because digitization of the grid system provides significant benefits like rich information at lower cost, greener energy, increased efficiency etc. Metering infrastructure plays an important role in the smart grid and acts as an important interface between utilities and its consumers. A metering network comprises a large number of different types of energy meters like advanced meters and legacy meters. To achieve the vision of smart grid, above said metering networks are integrated for exchanging the usage data and taking necessary control actions. Therefore, making grid digitization introduces lot of concerns about their security. To understand various security issues, this article discusses plurality of threats involved at different stages in the AMI system.

Keywords: AMI, energy meter, data collector, head-end

Volume 4 Issue 4 - 2018

Nitin Gupta
CPA Global, Patent Research Specialist, India

Correspondence: Nitin Gupta, CPA Global, Patent Research Specialist, India, Email nitin_ias@yahoo.co.in

Received: December 24, 2017 | **Published:** July 25, 2018

AMI security threats

Data sent by AMI components/modules can be called as a stream of packets, wherein data is sequentially continuous and larger in size than the device's memory, and most importantly mining algorithm can trace data for a very limited number of times.[1] For this reason, the nature of data in each component of AMI has been characterized in the Table 1. Figure 1 which shows that there exists plurality of entry points to enter any AMI network that need to be protected from vulnerability and thwarting attempts from insider and outsider users. At present, industrial meters have very limited amount of memory for necessary updates.[2] Therefore a smart meter's memory and processing capacity should be enhanced in order to provide it with enough security and protection (as well as other analytical capabilities). The security of AMI network is very essential because it is responsible for remote access of various smart home appliances, providing real-time pricing, energy usage recording etc. Apart from the advantages gained by integrating smart devices and applications of metering infrastructure as discussed in the previous sections, certain security threats[3–7] are always involved if such metering networks are operated without proper security measures. Specifically, there is always a fear in utility's and user's mind with following notions:

a. Authentication of real-time pricing information sent by the utilities,[8,9]

b. Correctness of metered information sent by electricity consumers,[10,11] and

c. Privacy of electricity consumers.[12]

Therefore, to provide a secured AMI architecture, it is necessary to understand various types of threats/actors involved that may cause the failure of entire AMI system and vision of the smart grid. Figure 2 & Table 1 summarize the possible attacks in the AMI network with respect to the type of security and the level of threat.

Conclusion

AMI provides ability to measure power consumption of users in real-time and on the basis of this information, it enables utilities to promote and involve the users in demand response program, provide them real-time pricing information, detect theft and lot of many other features. All such features are provided by use of remote internet network which in turn causes/invites inherent security risks for the utilities. Security measures are essential for any service provider. For achieving the vision of smart grid, such measures need proper attentions for providing significant benefits like secured rich information at lower cost, greener energy, increased efficiency etc. This article describes various security threats that can be associated at different stages of the AMI network and have been summarized in Figure 1 & Figure 2 and Table 1 & Table 2. This can help AMI solution providers and utilities in integrating the metering infrastructures securely.

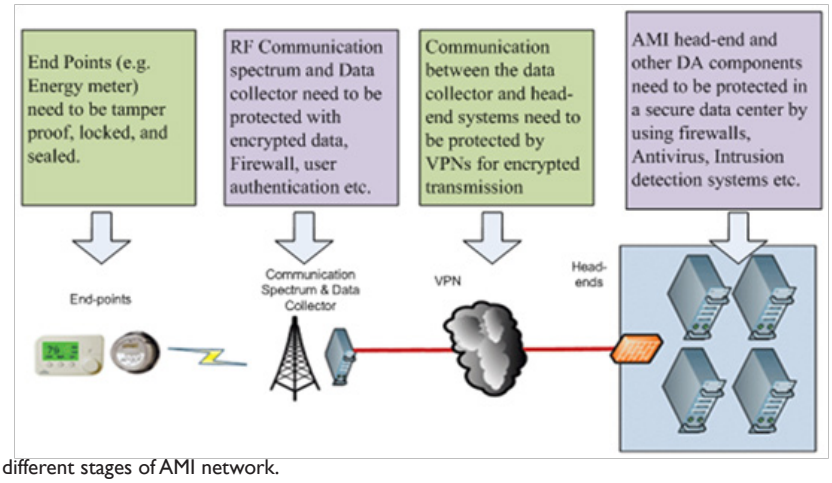

Figure 1 Security required at different stages of AMI network.

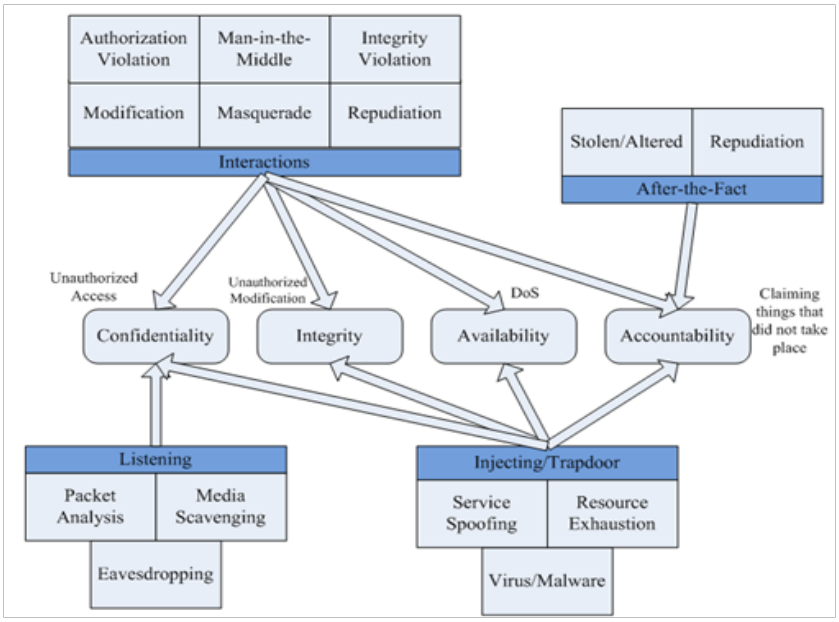

Figure 2 Relationship between threats and the security requirements.

Table 1 Characteristics of energy meter, data collector, and head-end application

Energy meter	Data collector	AMI head-end application
Meters installed in consumer premises produce data in small amount.	Data collector/concentrator receives data from hundreds or thousands of energy meters and is comparatively of high volume.	AMI head-end application, at top level, receives data from various data concentrators and being a top hierarchical node, the application process data of million energy meters.
Most of the energy meters comprise memory in the range of kilobytes with limited processing capacity.	Memory capacity of data collector is high and is in the range of Megabytes with more data processing capabilities.	The applications run on servers and possess high computation resources with a huge amount of memory.
Data speed is low because the generation of amount of data packets follows poisson distribution or data is polled non-frequently by concentrators.	Data speed is high as it aggregates data from hundreds or thousands of energy meters.	Data speed is comparatively very high as it handles energy meter data, commands, events etc.

Table 2 Quick glance at various threats in AMI system

Issue	Description	Security type	Level of threat
Listening/ Sniffing	Unauthorized users monitor the AMI Network communication by: Eavesdropping, Packet analysis,	Confidentiality	High
Modification/ Data Alteration	Unauthorized modification of captured AMI data by intercepting the data packets. This is called repudiation.	Integrity	High
Interactions	Interaction and interfacing of AMI with other systems invite unauthorized users to access to AMI components, modify data, DoS attack, and Non-repudiation.	Confidentiality, Integrity, Availability, and Accountability	High
Injecting code in AMI System	A malicious code/program injected in the AMI system invites unauthorized users to access to AMI components, modify data, DoS attack, and Non-repudiation.	Confidentiality, Integrity, Availability, and Accountability	High
Insider Attack	The insider attack take advantage of access to systems at the opposite end of the AMI system from the consumer endpoint.	Confidentiality, Integrity, Availability, and Accountability	Low-High

Acknowledgements

None.

Conflict of interest

The author declares there is no conflict of interest.

References

1. Michael Chau, Wei Thoo Yue, Alan Wang G, et al. Intelligence and Security Informatics. Pacific Asia Workshop; Kuala Lumpur, Malaysia. Springer; 2012. P. 207.
2. Shein R. Security measures for advanced metering infrastructure components. Proceedings of the Asia-Pacific Power and Energy Engineering Conference; China. 2010:1−3.
3. Ye Yan, Yi Qian, Sharif H, et al. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Journal of Communications Surveys & Tutorials*. 2013;15(1):5−20.
4. Chikuni E, Dondo M. Investigating the security of electrical power systems SCADA. IEEE AFRICON; South Africa. 2007:1−7.
5. Hauser CH, Bakken DE, Dionysiou J, et al. Security, trust, and QoS in Next generation control and communication for large power systems. *International Journal of Critical Infrastructures*. 2008;4(1/2):3−16.
6. Aditya Ashok, Adam Hahn, Manimaran Govindarasu. Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment. *Elsevier Journal of Advanced Research*. 2014; 5(4):481–489.
7. Ahmad Usman, Sajjad Haider Shami. Evolution of communication technologies for smart grid applications. *Elsevier Journal of Renewable and Sustainable Energy Reviews*. 2013;19:191–199.
8. Bekara Chakib, Thomas Luckenbach, Kheira Bekara. A privacy preserving and secure authentication protocol for the advanced metering infrastructure with non-repudiation service. Second International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies; 2012.
9. Daniele Gallo, Carmine Landi, Mario Luiso. (2013) Low cost smart power metering, IEEE International. Conference on Instrumentation and Measurement Technology; 2013:763–767.
10. Xiao, Zhifeng, Yang Xiao, David Hung-Chang Du. Non-repudiation in neighborhood area networks for smart grid. *IEEE Communications Magazine*. 2013;51(1):18–26.
11. Choi, Jaeduck. An efficient message authentication for non-repudiation of the smart metering service. IEEE First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI); South Korea. 2011:331–333.
12. Efthymiou C, Kalogridis G. Smart Grid Privacy via Anonymization of Smart Metering Data, First IEEE International Conference on Smart Grid Communications; 2010:238–243.