Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 July 2019 doi:10.20944/preprints201907.0067.v1

Analysis of Efficient and Privacy-Preserving Metering Protocols for Smart Grid Systems

Nishant Doshi

Department of Computer Science and Engineering,

PDPU, India

Doshinikki2004@gmail.com

***Abstract*— From ancient time, electric grid system developed as one way direction in which users get the electricity from generators to far end. However, it is not the consumer centric as its one way process and consumer have no way to communicate to the server. Thus, with the development of digital revolution, the grid converted to smart grid and meter converted to smart meter. In smart grid, the protocol follows the bidirectional way of communication with support of consumers in the system. Recently in 2016, Jo et al. proposed the scheme for smart grid system using privacy preserving model and claimed to be efficient and secure. However, in this paper we have analyzed the scheme of Jo et al. and proved that the scheme is vulnerable to Replay attack and afterwards shows the change in protocol to withstand against this attack.**

Keywords : multi Server; remote user; mutual authentication; attack

I. INTRODUCTION (*HEADING 1*)

From beginning of the revolution in technology, the prime requirement for fulfillment and success of it depends on the several required parameters. One of the prime parameter is electricity due to which the evolution of technology is possible and up till now furnishing in extreme speed. With evolution of technology, indeed need of converting energy in smart energy, grid to smart grid, meter to smart meter is become prime requirements. In Fig 1, we have given the traditional power grid system. This system is broadly divided into three phases i.e. power generation, transmission grid and distribution grid. In power generation phase, the power will be generated through various resources like conventional and non-conventional i.e. solar plane, coal plant, nuclear plant, oil plant etc. The power generated from earlier phase will be transmitted through various medium which range from meters to hundreds of kilometers in reality. Finally, the power reached to the end users i.e. residential users, commercial users, industrial users etc. This traditional model is used for several years. However, in this scenario, the end users have no control of asking demand and supply to the specific needs.

This problem lead to the concept of smart grid network in which several data control unit (DCU) is deployed which in turn contains smart meters. All these smart meters are initially gets registered with the trusted authorities as to provide the authentication. This phenomenon is pictorially depicted in Fig 4. The overall diagram of smart meter is depicted in Fig 3. The overall diagram of micro grid is depicted in Fig 2.

In this line, many researchers have proposed as well analyzed the smart meters using techniques like data mining, privacy preserving, machine learning, security etc. Readers can find the more details on this in [3-16]. Recently Jo et al. in [1], proposed the effective privacy preserving based scheme for smart grid and claimed to be secure too. However, in this paper we proved that the scheme is yet vulnerable to replay attack due to misuse of timestamp as given by the authors.

Organization of paper: in section 2, we have given the view of Jo et al scheme. In section 3, we have analyzed the scheme of Jo et al and proposed the changes in protocol to avoid the replay attack. In section 4, we have concluded with future scope in the smart grid. Finally, references are at the end.

© 2019 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 July 2019 doi:10.20944/preprints201907.0067.v1

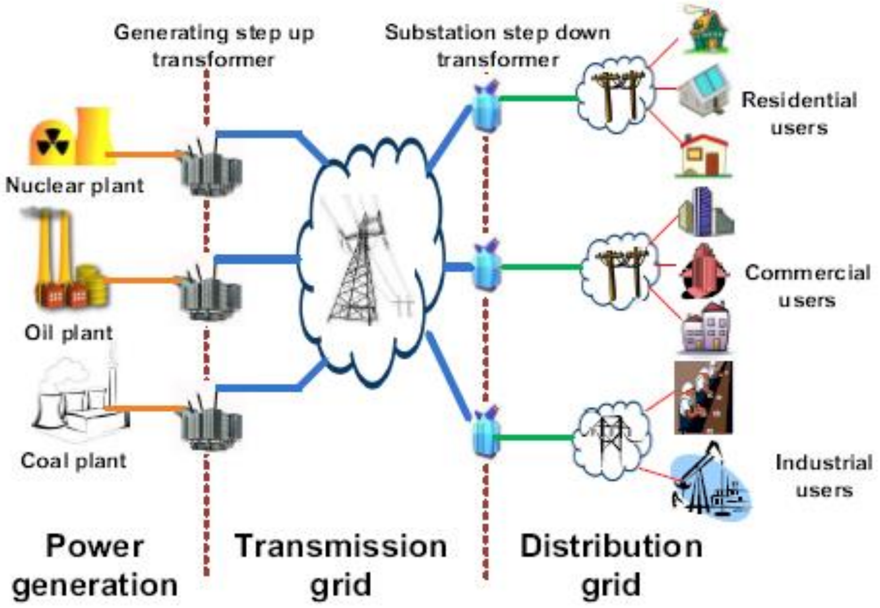

Figure 1 Traditional Power Grid [2]

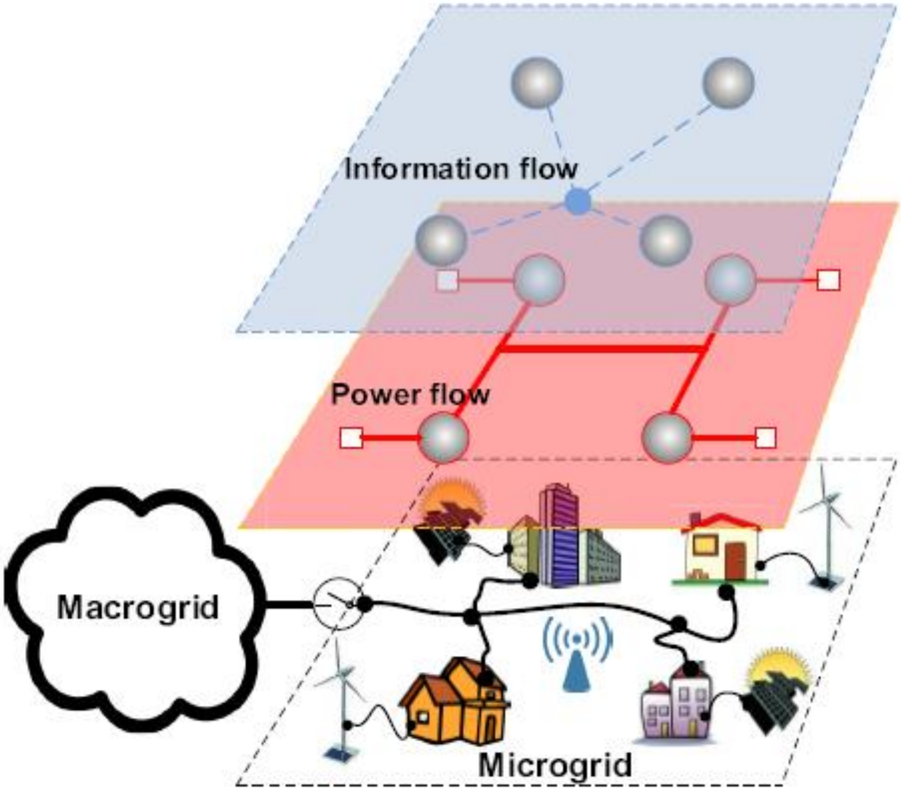

Figure 2 Simplified diagram of Microgrid [2]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 July 2019 doi:10.20944/preprints201907.0067.v1

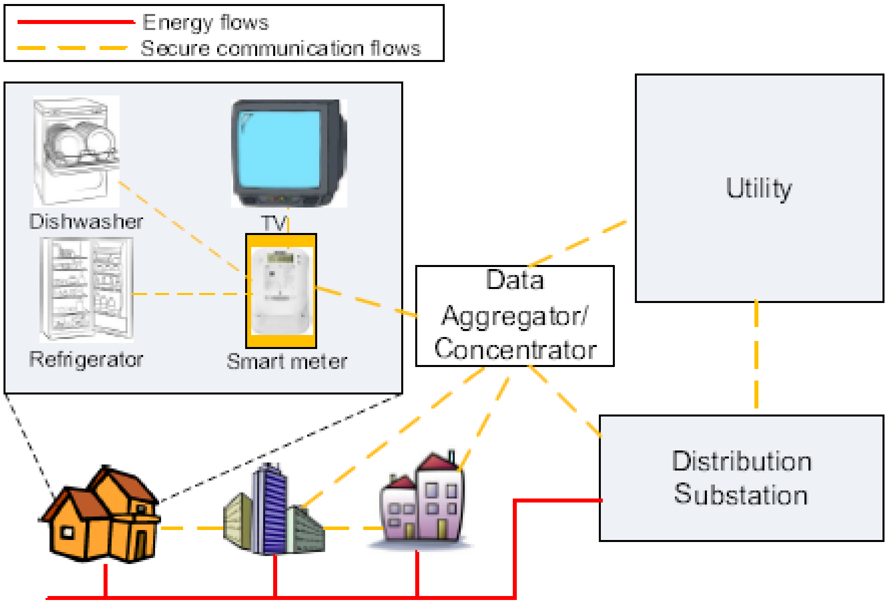

Figure 3 Simplified diagram for smart metering [2]

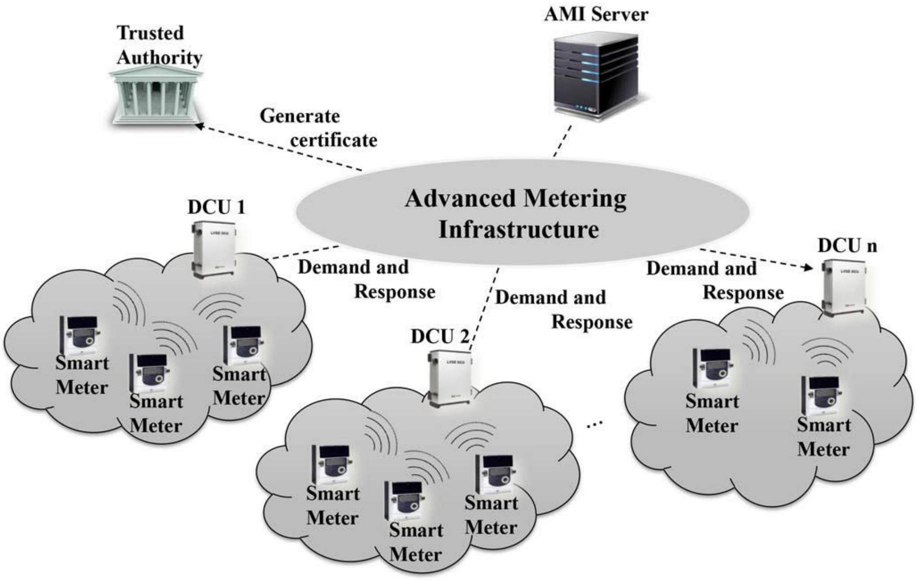

Figure 4 Smart Grid Network Model [1]

II. SCHEME OF JO ET AL.

The scheme of Jo et al is requires the following entities to interact and forward the communication i.e. Smart Meter i (SM_i), Data Collection Unit i (DCU_i) and Advanced Metering Infrastructure (AMI). The Fig 5, depicts the communication between these entities using public channel to communicate. The communications highlighted in red fonts are the one who can be replay.

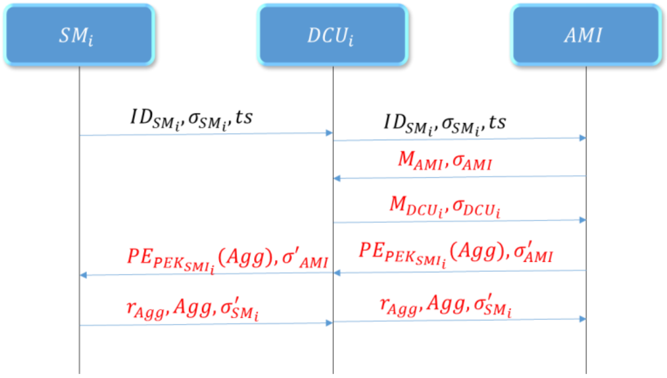
SM_i
DCU_i
AMI
$ID_{SM_i}, \sigma_{SM_i}, ts$
$ID_{SM_i}, \sigma_{SM_i}, ts$
M_{AMI}, σ_{AMI}
$M_{DCU_i}, \sigma_{DCU_i}$
$PE_{PEK_{SMI_i}}(Agg), \sigma'_{AMI}$
$PE_{PEK_{SMI_i}}(Agg), \sigma'_{AMI}$
$r_{Agg}, Agg, \sigma'_{SM_i}$
$r_{Agg}, Agg, \sigma'_{SM_i}$

Figure 5 Protocol by Jo et al [1]

III. Analysis

Recently, Jo et al. proposed an efficient and privacy preserving metering protocol for smart grid environment. In that paper, the authors have use the timestamp ts in protocol I within Phase 1. Afterwards, the same timestamp is used throughout the protocol I. Indeed, one can easily see that if messages of Phase 2 to Phase 4 can be repeated in future without any modification. The same can be seen in Fig5 with red font indicate the messages that can be repeated.

In Fig 6, we avoid this anomaly with security against replay attack by adding time stamp at every stage or say communication between any two entities.

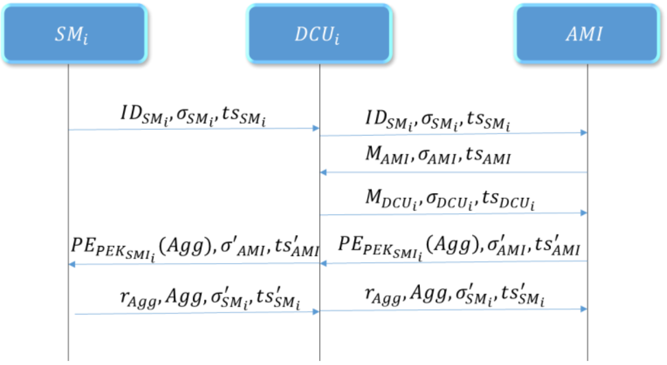
SM_i
DCU_i
AMI
$ID_{SM_i}, \sigma_{SM_i}, ts_{SM_i}$
$ID_{SM_i}, \sigma_{SM_i}, ts_{SM_i}$
$M_{AMI}, \sigma_{AMI}, ts_{AMI}$
$M_{DCU_i}, \sigma_{DCU_i}, ts_{DCU_i}$
$PE_{PEK_{SMI_i}}(Agg), \sigma'_{AMI}, ts'_{AMI}$
$PE_{PEK_{SMI_i}}(Agg), \sigma'_{AMI}, ts'_{AMI}$
$r_{Agg}, Agg, \sigma'_{SM_i}, ts'_{SM_i}$
$r_{Agg}, Agg, \sigma'_{SM_i}, ts'_{SM_i}$

Figure 6Proposed Approach

Indeed, as seen from Fig 6, with minor overhead in the protocol due to Jo et al. , it can be secure against replay attack.

Conclusion and Future Work

In this paper, we have explained the utilization of smart grid, smart meter as well as smart infrastructure to deploy the smart energy. We have taken the recent paper to analyzed and prove that it's susceptible to replay attack and afterwards give the update which can remove this problem. In future work, one can device the scheme having better performance as well as more secure as to its predecessors.

References

[1] H. J. Jo, I. S. Kim and D H Lee, "Efficient and Privacy-Preserving Metering Protocols for Smart Grid Systems," IEEE Trans. Smart Grid, vol. 7, pp. 1732-1742, May. 2016.

[2] Fang, X., Misra, S., Xue, G., & Yang, D. (2011). Smart grid—The new and improved power grid: A survey. IEEE communications surveys & tutorials, 14(4), 944-980.

[3] B. Brown et al., "AMI system security requirements," UCA Int. Users Group, U.S. Dept. Energy, Washington, DC, USA, Tech. Rep. UCAIUG: AMI-SEC-ASAP, 2008.

[4] IEC Smart Grid Standardization Roadmap, 1st ed., SMB Smart Grid Strat. Group (SG3), 2010.

[5] Y. Xiao, "Security and privacy in smart grids," Boca Raton, FL, USA: CRC Press, 2013.

[6] American National Standard for Protocol Specification for Interfacing to Data Communication Networks, ANSI Standard C12.22-2008, 2009.

[7] M. S. Choi et al., "A guide to design of security protocol for advanced metering infrastructure," in Proc. Int. Workshop Info. Sec. Appl. (WISA), 2011.

[8] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 675–685, Dec. 2011.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 July 2019 doi:10.20944/preprints201907.0067.v1

[9] S. Kim et al., “A secure smart-metering protocol over power-line communication,” IEEE Trans. Power Del., vol. 26, no. 4, pp. 2370–2379, Oct. 2011.

[10] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[11] H. Li et al., “EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2053–2064, Aug. 2014.

[12] S. Ruj and A. Nayak, “A decentralized security framework for data aggregation and access control in smart grids,” IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 196–205, Mar. 2013.

[13] F. Li, B. Luo, and P. Liu, “Secure information aggregation for smart grids using homomorphic encryption,” in Proc. IEEE SmartGridComm, Gaithersburg, MD, USA, 2010, pp. 327–332.

[14] D. Engel and G. Eibl, “Multi-resolution load curve representation with privacy-preserving aggregation,” in Proc. IEEE PES Innov. Smart Grid Technol. (ISGT), Lyngby, Denmark, 2013, pp. 1–5.

[15] F. D. Garcia and B. Jacobs, “Privacy-friendly energy-metering via homomorphic encryption,” in Proc. Int. Workshop Sec. Trust Manage. (STM), vol. 6710. Athens, Greece, 2010, pp. 226–238.

[16] Z. Erkin and G. Tsudik, “Private computation of spatial and temporal power consumption with smart meters,” in Proc. Int. Conf. Appl. Cryptography Netw. Sec. (ACNS), Singapore, pp. 561–577, 2012.