Retraction

Retraction: Authenticated Smart Meter Reading for a Secure Smart Grid (J. Phys.: Conf. Ser. 1916 012212)

Published 23 February 2022

This article (and all articles in the proceedings volume relating to the same conference) has been retracted by IOP Publishing following an extensive investigation in line with the COPE guidelines. This investigation has uncovered evidence of systematic manipulation of the publication process and considerable citation manipulation.

IOP Publishing respectfully requests that readers consider all work within this volume potentially unreliable, as the volume has not been through a credible peer review process.

IOP Publishing regrets that our usual quality checks did not identify these issues before publication, and have since put additional measures in place to try to prevent these issues from reoccurring. IOP Publishing wishes to credit anonymous whistleblowers and the Problematic Paper Screener [1] for bringing some of the above issues to our attention, prompting us to investigate further.

[1] Cabanac G, Labbé C and Magazinov A 2021 arXiv:2107.06751v1

Retraction published: 23 February 2022
Authenticated Smart Meter Reading for a Secure Smart Grid

Vineeth V V¹, Harikoushik A¹, Haripriya P¹, Harishankar A S¹, Dharshana C P¹
¹Department of Electrical and Electronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India. vineethvv@skcet.ac.in

Abstract. A secure system is proposed in order to authenticate smart meter reading for securing the overall smart grid communication. Compression based techniques are employed to prevent power reading by unauthenticated entities. Impersonation attacks are common in smart grid environment which cause drastic security issues along with economic issues. Compression along with authentication is studied here to weed out the potential threats raised by unauthenticated access. Hypothesis based testing analysis is done to differentiate intruder based signal and genuine signal. This could be applied to meter data more effectively and is thought to bring about low authentication issues concerned with smart meter data. So the increased threat level in smart meter communications in grid can be lowered efficiently by using compression and authentication and make the overall system secure.

Keywords: Smart Meter Reading, Compression, Authentication.

1. Introduction
Concerning Energy management, the problems that prevail are accuracy in metering, misuse of energy by theft and addition of fault data. Smart meters play a vital role in providing solution for existing problems. Many advancements have been made in recent times to overcome the existing difficulties but there are some advancements to be developed still for giving justice to end public in energy management. Among the existing issues, one issue is measuring the exact power consumed in particular zone as well in region. As of now, the distribution companies as well as departments are using manual reading of power consumption, graphic data reading and measurement through sms. Still there are drawbacks such as manual labour effort, error in data reading lack of transparency etc.

For the calculation of exact power usage of different appliances, power needed is large. To this problem, a solution is obtained by identifying individual power usage among total energy consumption value using power disaggregation methods. Yet, there is a problem still existing when the power signal is sampled. If the process is disintegrated, it increases the complexion as number of sampling gets increased. To meet out this issue, compression techniques are used. Many techniques are available such as gaussian approximation which uses nonlinear learning principle and Single value decomposition method which is used for the compression of energy signals. But still the complexity exists when it is implemented in terms of smart meter. A good solution should have good performance and less complexity. The implemented system uses compressive sensing for compression and authentication of smart meter data.

2. Literature Survey
The bulletin examines the implementation of Supervisory Control and Data Acquisition (SCADA) and its way of implementing by National Communication Systems (NCS) with the support of National security and Emergency preparedness (NS/EP) and implementation of CIP. It further examines the present and future scopes of using SCADA systems.[1]

The conventional Power system has lot of disadvantages to overcome such as energy mismanagement as well as energy misuse. The developments in field of Information technology made to develop the concept of Smart grid so that the conventional power system can be integrated with newly emerging technologies with a view to improve energy management thereby interlinking several grids in order to provide reliable energy distribution to consumers.[2]

The paper explains the functions and aspects of smart meters. It also provides basic types of smart meter communications such as radio frequency (RF) and Power Cable carrier (PLC) and the recent advances made in this field. [3]

3. Smart Grid Security Goals

Accessibility, integrity, confidentiality and accountability are the main goals of intelligent grid security.

• Availability: This purpose ensures that information can be accessed in a reliable and timely manner. Security solutions also support Data Collection, refinement and sharing.

• Integrity: Data must be reliable and accurate. To prevent malicious attacks and frauds, the information must be verified and must be free of fraud.

• Confidentiality: Data generated by the grid in large volumes must be collected, stored and analyzed. Sensitive data is entered in relation to customers and services. To prevent unauthorized access to sensitive information, care must be taken.

• Accountability: Proper care is required when disclosing sensitive information, so user interactions with programs are performed efficiently and effectively with specific users. That is, for the tasks that make the users of the smart grid responsible. Information must be kept so that it cannot be misled and integrity is maintained.

4. Existing System

Smart meters play a very vital role in smart grid environment by making the two way communication of energy data and related measurement and report data between grid and ordinary energy consumers. There are numerous challenges for a smart meter such as limited memory, bandwidth etc. In the existing system, smart meter collect the energy consumption data and aggregates this data which is then sent to data controller unit. This is not usually sampled or compressed. Even if certain systems employ sampling, compression may not be carried out. Attacks like impersonation attacks can cause serious performance issues in smart grid.

As shown in Figure 1, smart metering infrastructure communicates with the data controller unit which can be located near residential area’s electric poles. The data that is communicated to this unit includes energy consumption data, total cumulative power, timing related data, energy demand data etc. Considering the security of these data, all these communications are to be secured by means of techniques like compression. That is signals are to be compressed and applying a high sampling rate for the precise calculation of energy consumption data.
Compressive sensing based security standards are not widely used in existing systems. But it can be used to reduce the signal processing complexity and the effect of sampling and compression in smart meters. This has been used in certain systems for the residential power signals but is found to less effective.

5. Proposed System

The main idea of the system is compressive sensing based authentication and compression method to protect smart meter data. Rather than applying this method to residential energy signals, it is applied to aggregated energy reading and this is done based on an empirical model. A specialized measurement matrix is used for authentication in order to authenticate the energy signal and prevent unauthenticated intervention. This helps the data controller unit to discard the unauthenticated power signal (generated by an intruder) that it receives. This effectively reduces the network traffic by preventing the unnecessary signals generated by intruders in the network. This measurement matrix based method is found to have better performance compared to other existing methods [4-11].

The energy data signals that are transferred for smart meters are empirically modelled for analysis. By using this analysis, parameter values and distributional probabilities are found out. This is done by analyzing the collected data. Empirical calculations and analysis are done to represented values as sparse values with a definite matrix for representation. Modelling is done based on the collected data and appropriate transformation techniques are used to compress periodic signals. The system consists of two smart meters, one is a legitimate meter and another is an intruder meter. The data controller unit carry out initial checking and authentication based on cryptographic approach. It then creates a measurement matrix to check out whether the signal received by it is from an intruder meter or a legitimate meter. This is done by the compressive sensing based method of authentication. Thus a data controller unit can efficiently detect a signal form an intruder meter.

The paper thus brings about a novel approach for compression and authentication of meter data under transmission. Authentication is done effectively to avoid impersonation attack. The probability of error for authentication is the only probability of the data controller unit making a wrong choice during hypothesis testing.

6. Conclusion

Smart meters are an important component of smart grid and securing it is of great importance. This paper proposes a scheme that uses both compression and authentication in smart grid to avoid
impersonation attacks and other related attacks in a smart meter. Compressive sensing based compression is used to reduce the complexity of computation and to increase the performance. A hypothetical testing has also been done for theoretical analysis and authentication of energy signals.

References

[1] Boyer, S.A.. Scada: Supervisory Control And Data Acquisition. USA: International Society of Automation; 4th ed.; 2009. ISBN1936007096, 9781936007097.

[2] Wang, W., Lu, Z.. Survey Cyber Security in the Smart Grid: Survey and Challenges. ComputNetw 2013;57(5):1344–1371. URL: http://dx.doi.org/10.1016/j.comnet.2012.12.017.

[3] Chang, K.H., Mason, B.. The ieee 802.15.4g standard for smart metering utility networks. In: Smart Grid Communications (SmartGrid-Comm), 2012 IEEE Third International Conference on. 2012, p. 476–480. doi:10.1109/SmartGridComm.2012.6486030.

[4] Rottondi, C., Verticale, G., Capone, A.. Privacy-preserving smart metering with multiple data consumers.ComputerNetworks2013;57(7):1661713. URL: http://www.sciencedirect.com/science/article/pii/S1389128613000364.doi:http://dx.doi.org/10.1016/j.comnet.2013.02.018.

[5] Shamir, A.. How to share a secret. Commun ACM 1979;22(11):612–613. URL: http://doi.acm.org/10.1145/359168.359176.doi:10.1145/359168.359176.

[6] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.. Private memoirs of a smart meter. In: Proceedings of the 2Nd ACMWorkshop on Embedded Sensing Systems for Energy-Efficiency in Building; BuildSys ’10. New York, NY, USA: ACM. ISBN 978-1-4503-0458-0; 2010, p. 61–66. URL: http://doi.acm.org/10.1145/1878431.1878446.

[7] Lu, R., Liang, X., Li, X., Lin, X., Shen, X.S..Eppa: An efficient and privacy-preserving aggregationscheme for secure smart grid communications. IEEE Transactions on Parallel and DistributedSystems2012;23(9):16211631.doi:http://doi.ieeecomputersociety.org/10.1109/TPDS.2012.86.

[8] M. Suganya and H. Anandakumar, Handover based spectrum allocation in cognitive radio networks, 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Dec. 2013.doi:10.1109/icgce.2013.6823431.doi:10.4018/978-1-5225-5246-8.ch012.

[9] Haldorai and A. Ramu, An Intelligent-Based Wavelet Classifier for Accurate Prediction of Breast Cancer, Intelligent Multidimensional Data and Image Processing, pp. 306–319Chim, T., Yiu, S., Hui, L.C.K., Li, V.K.. Pass: Privacy-preserving authentication scheme for smart grid network. In: Smart Grid Communnications (SmartGridComm), 2011 IEEE International Conference on. 2011, p. 196–201. doi:10.1109/SmartGridComm.2011.6102316.

[10] Boneh, D., Lynn, B., Shacham, H.. Short signatures from the weil pairing. In: Proceedings of the 7th International Conference on the Theoryand Application of Cryptology and Information Security: Advances in Cryptology: ASIACRYPT ’01. London, UK, UK: Springer-Verlag.ISBN 3-540-42987-5; 2001, p. 514–532. URL: http://dl.acm.org/citation.cfm?id=647097.717005.