Fortifying Smart Meters with More Resilient Communication Protocols

CS3923/6814, Team 20
Liana Najaroen, Guanwei Zhang, Sahil Gupta, Brian Chuk

I. ABSTRACT

With the advancement in technology, we see conversion in devices to incorporating more software. Of course with the utilization of technology, it opens a new door for attackers and hackers who would be able to gain access to these devices. This paper focuses on smart electric meter and the security concern that arises from this implementation. Negative consequences that can result from poor security of smart electric meters include attackers gaining control of the device itself and violating the user's privacy due to the access of private information. This paper demonstrates different potential solutions that could prevent potential attackers. Potential solutions discuss in this paper includes the implementation of 4G LTE, bluetooth, encryption, and protocols.

II. KEYWORDS

advanced metering infrastructure, attack, authentication, cyber, data acquisition, electricity, encryption, GSM, network, protocols, security, smart meter, software, supervisory control, threat

III. INTRODUCTION

Smart Electric meters are the electronic digital devices which tracks the usage of electricity in households and transfer that information along with other customer details to the AMI(Advanced Metering Infrastructure) system. Smart meters have many potential benefits to offer to the customer and electricity company also. This includes an end to the estimated bills, better electricity regulation for customer, constant updates to the AMI, better management of electricity, automated power saving capabilities. A study conducted on the household electricity consumption on average is reduced by approximately 3-5 percent when experimented on the trials[1]. But when we consider the security issues with the smart electric meters, the concern grown even bigger than its benefits and usage. We will try to propose some solutions in the coming sections to prevent any cyber attack on the smart electric meters. In the next section we provide some background for the security issues and the past incident which roots from the compromise in the communication protocol that the smart grid uses to communicate with the electric meters.

IV. BACKGROUND

Although smart electric meters provide many benefits to the Advanced metering system to keep the track of the electricity consumption and customer behaviour to optimize and regulate the charges but with great power comes a great responsibility. A smart grid has four main components which are advanced metering infrastructure (AMI), supervisory control and data acquisition (SCADA), plug-in hybrid vehicle (PHEV) and communication protocols and standards. Smart meter is a component of AMI, which provides accurate measurement and automate remote reading of power consumption[2]. The AMI happens to communicate with smart meter through various Communication protocols. It could be PLC, DSL, WiFi, ZigBee, GSM/UMTS/LTE or even satellite communication. To be sure of the security of the system we gave to take care of at least 4 security concerns: confidentiality, integrity, availability and non repudiation.

For once leaving the software security and hardware/physical security aside, we will focus our study on the network security of the smart grid and what communication protocols are involved in the smart grid network to facilitate the data transfer from host to server or from host to host.

The most important attack impact is meter tampering. If the adversary gets successful in compromising the network of the smart grid, he/she could probably sniff on the communication channel, drop the packets received and send manipulated data to electricity company. It could result in the attacker to adjust the reading and send back the inflated bill. Mesh or wireless networks are able to be attacked by a malicious actor via methods such as personating mobile towers, authentication attacks, and encryption attacks on the traffic between the meter and the upstream relays or access points. As such, security design considerations need to include strong authentication and encrypted management of credentials.

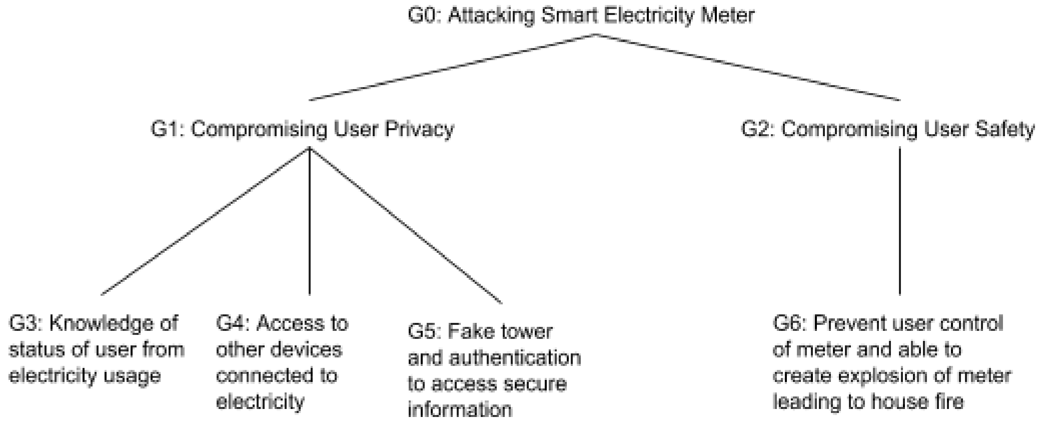
Our focus for this paper is how to secure the communication between AMI and smart grids. So essentially, when the communication happens between two parties, A and B, we need to make sure that the medium of communication is secret to both the parties, no one else is in involved in the communication and if tampered, there should be detection mechanism.

For all e to discuss and propose some solutions that can assure the network security to certain extent. The basic functionalities for network security we need to take care in the communication protocols are Encryption, Authentication and Intrusion detection.

Mostly all Smart Electric meters use GSM technology for communication or Zigbee protocol. To capture the data in GSM we use special devices like SIM boxes which operate on the same frequency. Once data been captured, GSM can be deciphered because it uses A5/1 stream cipher for the encryption over the channel. A5/1 stream can be easily decrypted using rainbow table attacks. Thus a better Encryption and Authentication method is needed to protect the communication. The another widely used protocol for communication is ZigBee Protocol (which is radio frequency communication). On a brighter side uses Strong AES encryption keys but its shortfalls in implementation can lead an attacker to gain control over the communication.

V. THREAT MODEL

In the previous paper, we developed an attack tree for smart meters. Let’s review the tree and look into how the original attack and how the security improvements under review address them.


G0: Attacking Smart Electricity Meter
G1: Compromising User Privacy
G2: Compromising User Safety
G3: Knowledge of status of user from electricity usage
G4: Access to other devices connected to electricity
G5: Fake tower and authentication to access secure information
G6: Prevent user control of meter and able to create explosion of meter leading to house fire

Threat	Solution Proposed by Designers
G3: Knowledge of status of user from electricity usage	Smart meter has built-in encryption to protect user data
G5: Fake tower and authentication to access secure information	The new 4G LTE connection will prevent this from happening
G4: Access to other devices connected to electricity G6: Prevent user control of meter and able to create explosion of meter leading to house fire	Using modern security protocols would prevent unauthorized access to the smart meter

VI. DESIGN

The proposed solution should provide a more secure smart meter with the following new features:

- Use of the 4G LTE network connection to communicate with the utility company
- Use of Bluetooth to communicate with other home devices

- Better Implementation and configuration of Zigbee protocol should protect the key at every node in the ZigBee Network. As the network key is the only way to authenticate the connection in the network.
- On top of the communication channel we should install either distributed intrusion detection system or centralized intrusion detection system. Distributed Intrusion Detection system is more effective for timely discovery and thus rapid and low cost recover from the attacks[3].
- Better security practices. Originally each smart meter built by the same company used identical passwords. It would be more secure for each smart meter manufactured to have individual passwords to be accessed
- Better physical design to prevent physical tampering

VII. IMPLEMENTATION

The first decision that we should make while implementing the network security for the communication channel is that which communication protocol should we choose? Which communication protocol is more secure in secrecy and privacy? Which one would be efficient and provide faster and reliable communication. Hereby some of the solutions that are proposed are as follows:

4G LTE is way secure than GSM/2g/3g in terms of authentication. Initially the host obtains the IP address which helps in communicating with the packet switched networks. This provides the host a communication over network layer. After establishing the connection, 4G LTE implements EPS-AKA authentication mechanism which is lot better than any other cellular wireless communication protocol. The encryption mechanism which 4G LTE uses is more difficult to crack than the encryption algorithms used by its predecessor communication protocols. The 4G LTE uses SNOW 3G stream cipher and the UEA2 confidentiality and UIA2 integrity algorithms.

For the short range communication between the smart electric meters and other IOT device in the household, it's better that we use bluetooth technology. Bluetooth 5.0 comes with 4 security levels and 2 security modes. You can run Secure Connection Only Mode with Secure Mode 2 instead of 1 to ensure all data is signed, but since the data is encrypted, and more math means more computing power, and more computing power means faster battery drain,

If we are using the ZigBee protocol the better implementation and configuration can result in the secure communication channel for AMI to communicate with smart meters[4].

- To avoid data tampering when detected, ZigBee should be pre-configured to erase any sensitive information or keys from the memory.
- Default TClink should not be used.
- Key establishment should be done via Out-of-Band channels.

- Network keys should keep changing regularly to avoid dictionary attacks.

After choosing the communication protocol and correctly doing the configuration of it for better secrecy and anonymity, we should further deploy the intrusion detection and intrusion prevention system. An effective IDS or IPS system will help avoid the attacker to gain control over communication based on the anomaly detection from behavioral pattern of customer. IDS should be able to protect the AMI from all three categories of attacks. 1) System Information, 2)Network Information and 3) Policy information.

VIII. EVALUATION

The overall design and proposed implementation suggest that existing smart meters will either have to be replaced or modified to support the new communication protocols and operating behaviors.

As discussed in the previous section, the use of 4G LTE is way more secure than GSM/2g/3g in terms of authentication. As Sebastian Banescu et al. [5] discussed in their paper, LTE is not vulnerable to the crypto-attack, since KASUMI cipher is no longer used by LTE. Although it remains vulnerable to both the DoS attack on the PS and the side-channel attack on the SNOW 3G protocol, LTE still has better security features than UMTS/3G, and of course than 2G.

The use of Bluetooth for short range communication protect the device from communication with unknown sources, i.e. potential attackers. Service-level security and device-level security work together to protect Bluetooth devices from unauthorized data transmission. [6] Security methods including authorization and identification procedures limit the use of Bluetooth services to the registered user and require users to make conscious decision to accept a data transfer.

ZigBee protocol itself may achieve good security performance. But as Xueqi Fan et al. pointed [7], the security depends on secrecy of the encryption may be breached during the key's initialization or distribution. So we suggested a better implementation and configuration to avoid mitigate such issues.

IX. RELATED SOLUTIONS

A. GPRS Security for Smart Meters

Martin Jaatun et al. [8] provided an overview of the security of GPRS related to its use for AMI and recommended the use of UICC/USIM instead of the SIM as this offers stronger and more extensive authentication and encryption.

In their solution, authentication of smart meter terminals to the communication network is performed by GPRS, and the GSM- Milenage implementations of the A3 and A8 algorithms is thus recommended for authentication mechanism used. GPRS communication sent on the wireless link is encrypted but terminates in the core network. So they recommended CEA3 or above for encryption, and NDS/IP for protection of the GTP traffic, are recommended in the GPRS core network. They also recommend that DSOs use VPN solutions to protect the data sent to and from the smart meters. However, GPRS doesn't offer mechanisms to prove actions. Attacks such as deny of service may still need to be prevent relying on additional security added on the application layer.

B. Key Management Scheme for Secure Communications of AMI

Nian Liu et al.[9] proposed a novel KMS to solve the key management problems of AMI systems. For key Generation, a user key and a group key are generated by using a secure random key generation function. A session key is created based on a user key or group key and mixed with additional value using hash.

For key freshing, the user key can be auto refreshed in a certain period, and group keys refreshing depends on if there are users joining or quitting DR project. Both user and session keys use hash on refreshing methods.

For authentication and integrity, session keys are held only by the two communication ends. The receive will verify the signature of encrypted data first with a secure key.

For forward and backward security, if there are any users joining or quitting the group, all group keys and additional values will be regenerated, refreshed and distributed to members of the new group.

C. Security Protocols

Fatemeh Halim et al.[10] claimed that communication perform by smart meter must use secure protocols such as IPSec, SSL, TLS, and SSH, etc. They also pointed that the smart meter gateway can support intrusion prevention systems and packet filtering (Firewall) which can monitor and filter the network traffic.

D. Integration for communication and utility ICT

Vilmar Abreu et al.[11] worked on an integral solution for secure communication between smart meters and the utility ICT (Information and Communication Technology). They ported an RTOS code to a SM based on an 8051 μC and adapting it to support an MLSM (Multi-Level Security Mechanism). The MLSM embeds a multilevel integrity mechanism based on the BIBA model, aiming to provide the hardware-equivalent secure mode in software-level, supported by the RTOS.

X. CONCLUSION

The implementation and negative consequences concerning security of smart electric meters was briefly discussed in this paper. Following, the importance of the increase in security around smart meters was emphasized due to the negative events that can occur once attackers gain access into the device. Different improvements to the security of smart meters were explored further such as securing communication between the device and company through encryption, authentication, and intrusion detection. ZigBee protocol was classified as improving the communication due to strong AES encryption keys, however does little to prevent attackers gaining access. Due to this, 4G LTE was explored and it was concluded that it is more difficult to crack due to more advanced encryption algorithms. Bluetooth was also explored but due to its tendency to drain the battery, the finding was that 4G LTE was the superior communication protocol.

XI. REFERENCES

[1] McKerracher, C. and Torriti, J. (2013) Energy consumption feedback in perspective: integrating Australian data to meta-analyses on in-home displays. Energy Efficiency, Volume 6 (2). pp 387-405 [1]

[2]Fatemeh Halim, Salman Yussof and Mohd. Ezanee Rusli"Cyber Security Issues in Smart Meter and Their Solutions "IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.3, 2018

[3]Alvaro A. Cárdenas, Robin Berthier, Rakesh B. Bobba, Jun Ho Huh, Jorjeta G. Jetcheva, David Grochocki, and William H. Sanders"A Framework for Evaluating Intrusion Detection Architectures in Advanced Metering Infrastructures"IEEE TRANSACTIONS ON SMART GRID, VOL. 5, NO. 2, MARCH 2014

[4]https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

[5] Banescu, Sebastian, and Simona Posea. "Security of 3G and LTE." Faculty of Computer Science, Eindhoven University of Technology.

[6] Curt Franklin, and Julia Layton. "How Bluetooth Works - Bluetooth Security" https://electronics.howstuffworks.com/bluetooth4.htm

[7] Fan, Xueqi, et al. "Security Analysis of Zigbee." (2017).

[8] Jaatun, Martin Gilje, Inger Anne Tøndel, and Geir M. Køien. "GPRS Security for Smart Meters." *International Conference on Availability, Reliability, and Security*. Springer, Berlin, Heidelberg, 2013.

[9] Liu, Nian, et al. "A key management scheme for secure communications of advanced metering infrastructure in smart grid." IEEE Transactions on Industrial electronics 60.10 (2013): 4746-4756.

[10] Halim, Fatemeh, Salman Yussof, and Mohd Ezanee Rusli. "Cyber Security Issues in Smart Meter and Their Solutions." IJCSNS 18.3 (2018): 100.

[11] Abreu, Vilmar, et al. "A smart meter and smart house integrated to an IdM and key-based scheme for providing integral security for a smart grid ICT." Mobile Networks and Applications 23.4 (2018): 967-981.