Privacy Assuring Protocol using Simple Cryptographic Operations for Smart Metering

Waleed Akram Baig , Faraz Idris Khan, Ki-Hyung Kim and Seung-Wha Yoo

Department of Information and Computer Engineering
Ajou University, Suwon, South Korea
{waleedbaig, fikhan00, kkim86, swyoo} @ajou.ac.kr

Abstract

The next era is foreseen to revolutionize the utility application with the technological advancements in IT and telecommunication. Intelligence will be seen in industrial machines equipped with embedded technologies enabling communication using low power wireless technology. Smart meter has recently gained lot of attention from the research community as this has raised unique challenges especially w.r.t security. Privacy preservation in such an environment is discussed to be critical as it may lead to devastating effects or even blackout which has been witnessed before. In this paper, we propose a privacy preserving algorithm which ensures resiliency against credentials theft with cryptographic operations where they are transported in a secure manner. We evaluated different encryption algorithms RC5, MD5, SHA1 in terms of computational and communication resources consumed by them in the proposed privacy preserving algorithm. In future, extensive evaluations and proofs of cryptographic algorithms will be included.

Keywords: *Privacy, Wireless Sensor Network Security, Public Key Infrastructure, Smart Grid Security, Smart Metering Cyber Security, Secure Payment*

1. Introduction

In the near future, advances in IT infrastructure have broadened its horizon to utility management system. As an example, Smart metering application which collects electricity usage in real time and periodically report them to collector devices in the neighborhood. The collector transports the aggregated data to the control centers for pricing. There is a chance that data at any point of the collection process might get modified, dropped, eaves dropped or forged which affects the pricing. In addition, there is a risk of overwhelming the metering network resources often termed as LLN (Low Power and Lossy network) characterized by resource constraints. It can be inferred that security schemes for such nature of network should be lightweight with low computational and communication cost. In literature, we encounter some efficient schemes as in [1] where data in batch is authenticated using cryptographic techniques from network security. Moreover, privacy is indicated to be of prime concern in Smart Grid deployment [2]. Revealing meter reading data leaks personal information. This exposes customer habits and behaviors which assists the agent in making decision and launching devastating attacks destroying the network. DoS attack is one such kind of attack where eaves dropped data can be replayed elsewhere exhausting network resources.

Recently, Wireless Sensor Networks has gained widespread attention over the years. It is considered to be one of the hot candidates over the years for various industrial applications i.e. process monitoring, industrial automation. Lately, it is been considered for Smart metering network where meters will be equipped with sensors assisting in collecting and aggregating data in the network [3]. Preserving privacy in WSN is already indicated to be an area that needs acute attention from the researchers as mentioned in [4]. WSN paradigm works in a similar fashion as that of Smart metering network as they collect, transmit and analyze the aggregated data. Privacy is indicated to be of concern especially for

applications like medical monitoring application which monitors patient's parameters like blood pressure, sugar level of critical privacy concern [4]. In [4], a comprehensive taxonomy can be found where the privacy preserving issue is classified into Data oriented privacy protection (protection of private data) and Context oriented privacy protection (protects location of data source and base station). The preserving techniques for WSN can be found feasible to implement in smart metering network due to its similarity. Data oriented privacy protection schemes which in summary ensure privacy of the aggregated data at various levels is quite relevant to AMI.

Security is a critical issue in a modern smart metering application. In case, of a common attack if a third party learning the behavior of the customer maliciously can use the information to achieve their own objective. It is important that the supplier should ensure the trustworthiness of consumption profiles. There is a chance that with the alteration of profile the output of the billing system results in a lower or higher value. This leads to a desire need of a whole security system constituting of cryptographic algorithms which signs and verifies the collected data at various stages of the collection process. One such work can be found in [5] where authors have proposed a plugin privacy component that acts as a mediator between the metering network and the system at the control center billing on the basis of the collected data. The suppliers ensure the integrity of the generated bill with some proposed operations signed data and tariff to come to the conclusion that the bill is to be trusted.

The contribution of our work can be summarized as

A resilient privacy preserving algorithm for smart metering application preventing malicious server from stealing credentials by applying cryptographic operations on the messages being transferred in the setup phase

2. Literature Review

Smart Grid security has received tremendous attention from the researchers since its realization is envisioned in a decade. Security issues in smart grid can be found in [11] where authors tried to identify open problems and issues. Still a complete security framework is not to be found in literature that ensures CIA (confidentiality, integrity and availability) for a smart grid IT infrastructure. Authentication in smart grid can be found in [1]. A desire need of light weight authentication protocol is desired work in this domain can be found in [5]. Apart from authentication, key management is largely an untouched area of research in Smart Grid which should be lightweight. Work in this domain can be found in [6]. In summary, the architecture has a trusted third party known as trust anchor with cryptographic algorithms such as elliptic curve public key cryptography, Needham-Schroeder protocol ensuring resilience against attacks like man-in-the-middle attack and replay attack.

In Data oriented Privacy, two kinds of adversaries have been identified; external and internal. Prevention can be found in [4]. In the domain, of context oriented privacy techniques the proposed techniques are flooding [7], Random walk [8], dummy injection [9] and fake data sources [10].The main overhead in such techniques is of power consumption due to additional traffic or injection of real data. The last kind of privacy mechanism called as temporal privacy where the attack scenario in this case happens when an event is generated and sensed at a particular time which if predicted could lead to prediction of target's next move in case of target tracking. Counteraction as proposed in [11] when the data is locally buffered for a random period at intermediate sensors along the routing path and adversary cannot estimate the original generation time of message.

More privacy preserving work can be found in [12] where a privacy aware framework is proposed and a technique in [13] does computation by multiple parties computing sum of consumption. We conclude, this section by arguing that there is very little work to found in the domain of smart metering privacy catering wide range of attacks.

3. Smart Metering Payment

The steps for smart metering payment protocol can be summarized in the following steps

- Setup phase

  During the setup phase the protocol begins with the key generation process to sign the policies which are to be followed to proceed with the payment. These policies once signed have to be verified later with the entities in the network.

- Meter usage
  In this stage the meter usage is collected using a protocol which consumes low resources from the network. These usage values have to be verified by the security credentials generated during the setup phase.
- Payment
  The payment is usually activated after a certain interval or period which is processed according to the policy. There is a chance of misuse during this phase as it is one of the critical one requiring extra cryptographic operation.

Figure 1 shows the smart metering payment protocol flow.

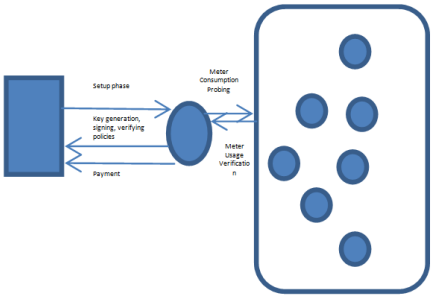

Figure 1. Smart Metering Payment Protocol

4. Attack Model

In this section, we present our attack model that we consider for the proposed protocol in this paper. We assume the meters are equipped with IEEE 802.15.4 radio running on 802.15.4 protocol. During the setup phase there is an assumption of a malicious server that compromises the security credentials from the provider server providing service to the smart metering network. The meter usage data get aggregated and reaches the service provider server where the payment matters are handled. In a case, when security credentials are compromised the malicious server can impersonate as a provider server and redirects the payments towards itself. This can happen once the policies are signed by the compromised credentials or by the malicious server generated untrusted certificates. These attacks can be classified as credential stealing attacks or man in the middle attack. One of the latest works on credential stealing can be found in [14]. Work on man in the middle attack where the authors have focused on an issue of energy theft in AMI and proposed a solution with additional overhead of authentication in the initial stages [15]. Figure 2, shows the flow of a scenario where credentials are being stolen by the malicious server. The existing privacy preserving schemes during the setup phase don't cater this scenario it begins with the key generation process then policies are signed with those keys. There is a need of additional cryptographic operation or security transaction that provides resilience against credential theft.

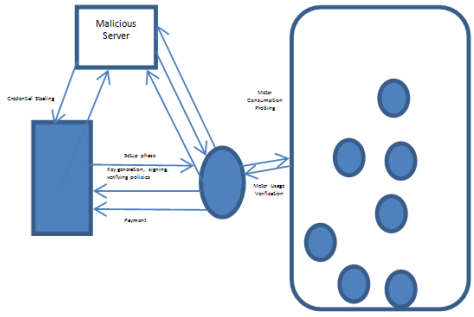

Figure 2. Credential Stealing Protocol Work Flow

5. Privacy Preserving Scheme

The privacy preservation scheme works as follows

- The provider begins by generating the policies *p* for payment and the key generator at the provider generates the keys by $KeyGen_p(seed)$ given a seed value a pair of keys is generated $(PubK_p, PrivK_p)$. $KeyGen_u(seed)$ we get $(PubK_u, PrivK_u)$ and with $KeyGen_m(seed)$ we get $(PubK_m, PrivK_m)$. The pair of keys will be used to hide the data being transmitted from the provider another $KeyGen_{encrypt}$ is used to generate $(PubK_{encrypt}, PrivK_{decrypt})$. The key pair $(PubK_{encrypt}, PrivK_{decrypt})$ is used to encrypt the communication of credentials in a secure way. For the sake of simplicity we make an assumption that the keys are broadcasted in a secure way as in [16]. Policy in the whole paper defines as a mapping of consumption, price and administrator defined policies for the metering network which can be represented by a tuple $(consumption, price, administrator_{policy})$. This ensures that the policies are transmitted in a secure way without being revealed to any one beside the concerned entities in a network. Then at provider side if the encryption function is represented by $E_{encrypt}()$ taking two input the key K and message m to encrypt we have

$$Encry(Keys) = E_{encrypt}(PubK_{encrypt}, PubK_p)$$
$$Encry(Policy) = E_{encrypt}(PubK_{encrypt}, P)$$

Similarly, this happens for the user and meter end then at the user end

$$Decryp(Keys) = D_{decrypt}(PrivK_{decrypt}, Encry(Keys))$$
$$Decryp(Policy) = D_{decrypt}(PrivK_{decrypt}, Encry(Policy))$$

- The encryption operation will make sure that the malicious server is unable to get hold of the security credentials generated in the start. This is made sure with keys being broadcast in a secure manner preventing from adversaries to get the keys.

$$S(M) = Sign(PubK_m)$$
$$V(M) = Verify(PrivK_m)$$

- By following the policies being signed and verified by the keys bill is generated by the provider which is followed to make a payment to the provider. All these transaction happens with the secure keys that were encrypted and broadcasted in the initial stages.

$$S(P) = Sign(PubK_u)$$
$$V(P) = Verify(PrivK_u)$$

Our proposed protocol introduces extra secure operation in the setup phase. This comes at the cost of extra cryptographic operations, computation and communication. Details of cryptographic operations and their proofs are left as a future work. The algorithm is shown as below.

Setup Phase

1. Key Generation Process ()

$$KeyGen_p(seed) = (PubK_p, PrivK_p)$$
$$KeyGen_u(seed) = (PubK_u, PrivK_u)$$
$$KeyGen_m(seed) = (PubK_m, PrivK_m)$$
$$KeyGen_{encrypt}(seed) = (PubK_{encrypt}, PrivK_{decrypt})$$

2. Secure broadcast of $KeyGen_{encrypt}(seed)$
3. Encryption and Decryption process at the Provider

$$Encry(Keys) = E_{encrypt}(PubK_{encrypt}, PrivK_p)$$
$$Encry(Policy) = E_{encrypt}(PubK_{encrypt}, P)$$
$$Decryp(Keys) = D_{decrypt}(PrivK_{decrypt}, Encry(Keys))$$
$$Decryp(Policy) = D_{decrypt}(PrivK_{decrypt}, Encry(Policy))$$

Meter Usage Phase

Signing and Verification at Meters

$$S(M) = Sign(PubK_m)$$
$$V(M) = Verify(PrivK_m)$$

Payment Phase

Signing and Verification of Payments at the provider

$$S(P) = Sign(PubK_u)$$
$$V(P) = Verify(PrivK_u)$$

Figure 3. Privacy Preserving Algorithm

6. Performance Evaluation

In this section, we will discuss the performance evaluation of our proposed resilient protocol. We summarize the configuration of our smart metering network and smart meter architectural design in table 1 and table 2 respectively.

Table 1. Smart Metering Network Configuration

Networking Standard	802.15.4
Data Rate	250Kbps
Modulation Scheme	BPSK
MAC protocol	CSMA/CA

Table 2. Smart Meter Configuration

Microcontroller type	ATmega88
Device Core	AVR
Data Bus Width	8 bit
RAM	SRAM 1KB byte
ROM	EEPROM 512 byte
Master Clock Frequency	128kHz
Instruction Set Architecture	RISC

We represent the computational cost as execution time for a certain block of data block where a = 352114 and b = 40061for RC5, a = 60980 and b = 458660 for SHA1 and a = 203656 and b = 86298 for MD5.

$$T(length)_{exec} = \frac{a + (b * \frac{length}{bksize})}{clock\_rate * bus\_width} \quad (1)$$

We represent the cost in terms of number of messages. Also we are assuming ECC 256 algorithm as a key generation algorithm. Communication cost for a given message length for the encryption algorithms can be calculated as

$$C(E) = n * \frac{m}{d} + \frac{k}{d} + \frac{policy}{d} + \frac{consumption}{d} + \frac{payment}{d} \quad (2)$$

E= Type of Encryption algorithm used to encrypt the keys
m = Size of Encrypted keys used for message communication between the provider and the user to be broadcasted
k = Size of encrypted keys to decrypt the policies
policy = size of encrypted 4 byte policies
consumption = size of encrypted consumption data
payment = size of encrypted payment data
d = data rate of a network
a = initialization overheads
b = time spent in operations repeated for each block

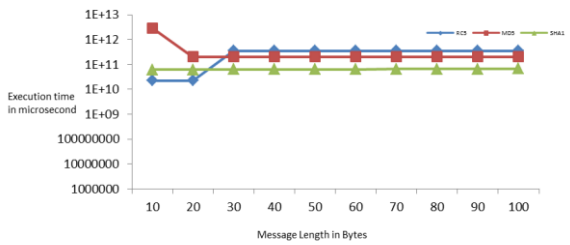

Figure 4. Computational Cost of the Encryption Algorithms

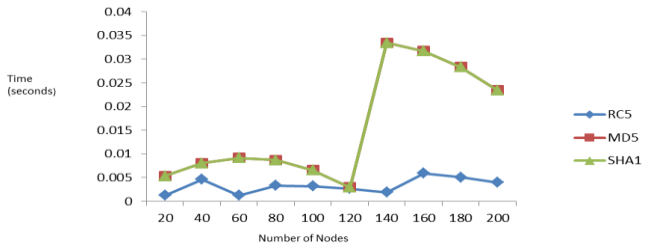

Figure 5. Communication Cost

From Figure 3, it is evident that all the encryption algorithms eventually reaches to steady state in the three of the hot candidates SHA1 takes lower execution time hence better suited to be used for encryption in the proposed privacy preserving protocol. In Figure 4, it is obvious that RC5 shows a stable behavior and low communication cost as compared to other algorithms. The difference is observed to be huge. And, MD5 and SHA1 show the same behavior. We conclude, by saying that from the designer's point of view he would have to take care of the trade-off in a scenario if optimal communication cost is desired then RC5 is the recommended option for the protocol. On the contrary, if computational resources are important then it would be better to choose SHA1 for the algorithm. We plan, to investigate the protocol extensively with experiments and proofs of the cryptographic algorithms.

7. Conclusion and Future Work

In this paper, we have proposed a more resilient privacy preserving protocol for Smart Metering infrastructure. A typical smart metering payment protocol in general works in three phase: setup phase, meter data usage phase and payment. Furthermore, we devise an attack model where a malicious server can steal security credentials and impersonate to force the customers to pay it. A privacy preserving algorithm is proposed which provide resiliency by using the keys generated at the setup phase where the key used for encryption is broadcasted securely to the users. This step ensures secure transaction later on with payment made to authentic provider server. For future work we plan to look into suitable lightweight cryptographic algorithms and with the derivation of their proofs. Furthermore, we plan to look into tradeoffs when providing resiliency and ensuring light weight algorithm.

References

[1] D. Li, Z. Aung, J. Williams and A. Sanchez, "Efficient Authentication Scheme for Data Aggregation in Smart Grid Fault tolerance and Fault diagnosis", IEEE Power and Energy Society Conference on Innovative Smart Grid Technologies (ISGT'12), 1-8 **(2012)**.

[2] A. Rial and G. Danezis, "Privacy-preserving smart metering", In: Proceedings of the 10th annual ACM workshop on Privacy in the electronic society *(WPES '11)*. ACM, New York, NY, USA, pp. 49-60 **(2011)**.

[3] 1888 Press Release, http://www.1888pressrelease.com/wireless-sensor-networks-in-smart-meters-a-market-with-unc-pr-326861.html.

[4] Jawurek, Marek, Johns, M. Kerschbaum, F. Fischer-Hübner, S. Hopper, Nicholas. In: The Physiology of the Grid: Plug-In Privacy for Smart Metering Billing. Privacy Enhancing Technologies, LNCS, (2011), Springer Berlin / Heidelberg.

[5] A. S. K. Pathan, "Security of Self-Organizing Networks: MANET, WSN, WMN, VANET", CRC Press **(2011)**.

[6] K. Yagnik, S. Vadhva, R. Tatro and M. Vaziri, "California Smart Grid Attributes: California Public Utility Commission Metrics", In: IEEE-Green, pp. 1-6, **(2011)** April.

[7] D. Boneh and M. Franklin, "Identity-based encryption from Weil pairing. In: Proc. of Crypto", LNCS 2001, vol. 2139, pp. 213-229 **(2001)**.

[8] T. Baumeister. "Literature Review on Smart Grid Cyber Security In: Technical Report", University of Hawaii, **(2010)**.

Authors

Waleed Akram Baig received a B.S. degree in IT from NUST Pakistan in 2005. He acquired M.Sc from the University of Greenwich, UK In 2007 and joined GC Uni. as lecturer. In 2008, He joined Ajou Ajou University, Korea as a Ph.D. Candidate. His research interests Security in Wireless Sensor networks, Smart Grid, and M2M.

Seung-WhaYoo is professor in Ajou University.

Faraz Idris Khan received his BS from NUST, MS from Kyung Hee University and pursuing his PHD from Ajou University South Korea. His research interests are Protocol and Network performance analysis, Routing protocols, Network Security. The domain of research span Wireless Sensor Networks, M2M, Smart Grid.

Ki-Hyung Kim received the B.S. degree in electronics engineering from Hanyang University, Korea. Later he acquired M.S. and Ph.D. degrees both in Electronics Engineering from KAIST, Korea. He joined Yeungnam University as an associate professor in 1997, wherein he served till 2004. During the professorship, he also joined AdForce, Inc in Cupertino, California, USA as a senior engineer in 2001.His research interests include wireless sensor networks, mobile ad-hoc networks, distributed systems design, and mobile embedded systems. He is an active contributor in the 6LoWPAN community that works towards interoperability of IEEE802.15.4 networks and IPv6 Internet. Currently, he is professor at Ajou University, Korea.