International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Secure Key Distribution Protocol with Smart Meter

Navneet Agrawal†*

†Department of Computer Science Engineering, Mahatma Gandhi Mission College of Engineering, Nanded, Maharashtra-431601, India

Accepted 30 Sept 2015, Available online 10 Oct 2015, **Vol.5, No.5 (Oct 2015)**

Abstract

Authentication is crucial for large and distributed systems, such as cyber-physical infrastructures. The focus of this paper is on the secure key distribution must be secure enough to any attempts to compromise the system. we first overview the key management scheme how probabilistic argumentation is applicable to modern public-key cryptography as an relevant gadget to evaluate webs of trust. We analyzed the arithmetic complexity of several procedures for generating RSA keys, choose the most e_cient of each, and did implementations in Java.

Keywords: *Security, Smart grid, Key management.*

1. Introduction

Smart grid, designed to replace common electric power infrastructure, is capable of making the grid work more efficiently, securely and decent through bidirectional flows of power and communication. A remote user authentication scheme requires low-computational and less communication cost, and provide mutual authentication. Although, the scheme does not maintain a verification table, the smart meter must maintain a table to store the users' *ID* to check its validity. In cryptography, key distribution is the function that hand over a key to two parties who wish to communicate with each other. The strength of any cryptographic system wait on Key distribution. Therefore, it is really important to have a secure key distribution system because if an attacker ever prevails in gaining access to the secure or private key, then he can compromise the whole system (S. William *et al*, 201).

A key factor in subscribe the Smart Grid problem is a decomposition of the power system and underlying standards and technologies into coherent parts that allow targeted research to be applied, while exposing the problems that have precluded solution development.

Following this, the Smart Grid problem is decomposed into four key areas: Generation, Transmission, Distribution, and Consumer. This will clearly delineate the areas of impact as well as expose the seams between systems where more investment is needed to develop the standards and best practices necessary to link up Smart Grid technologies.

For the symmetric key method, it is risky if all of the devices use one same preloaded key since if one of these devices is compromised the attacker could know every device's shared key in Key distribution by symmetric encryption means that the two parties who want to interchange encrypted data must share the same key. Instead of a preselected key, it is better to setup a trusted third party to distribute the shared key between two parties. The Kerberos system can be used in this environment to distribute the key for the components in the smart grid, however, the key distribution center (KDC) in the Kerberos system cannot support to distribute the keys when network or power outages happen. More importantly, it is unfabled and insecure to have a back-up server for the KDC considering the size of the smart grid.

The results have shown that the proposed scheme is scalable and strong competitors to pure symmetric key schemes, yet, it maintains all security levels provided by public key schemes. a symmetric key cryptosystem is appropriate for communication between the device, though a pre-installed system wide symmetric key or pair-wise keys stored on the devices are not suitable for reasons of security and lack of memory respectively.

2. Literature Review

The issue of key management for the smart grid has been broadly studied recently. Existing scheme proposed a new key management for the smart grid (Z. Cheng *et al*, 2005). In their scheme, they combine both of PKI and a third trusted anchor, which will essentially increase the complication for the smart grid because their protocol at least needs two different kinds of servers for public key infrastructure and the trust anchor respectively. Apart, this method is not secure against the man-in-the-middle attack which will be

*Corresponding author: **Navneet Agrawal**

shown in Investigation of Security which is in next section.

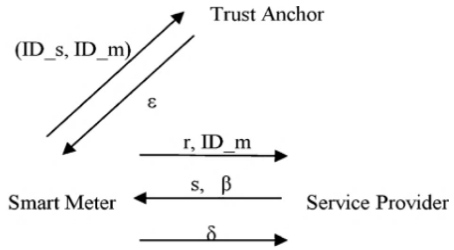
Recently, Metkle and Ekl have described By building on knowledge, solutions, and standards from Other systems and industries, the best security solutions can be utilized for each portion of the smart grid communications network. Clearly, Internet-based protocols (), but they still need many following steps to fully achieve their vision. It means that the smart meter is strictly required to handle these packets and it is a high-level requirement for current smart meters. In our paper, we will propose a secure key distribution protocol for the smart meters including a trusted third party in a non-PKI environment.

Zheng proposed signcryption based key transport protocols termed as Direct Key Transport Using a Nonce where nonce is an identity assigned by random number and DKTUTS (Direct Key Transport Using a Time-Stamp) over an ATM network where the protocols are compact, efficient and authenticated key establishment ones with the properties of short packet non-repudiation.

2.1 Organization of This Paper

The rest of the paper is organized as follows. In Section II, reviews of the existing key distribution scheme will also be pointed out. In Section III, the detail and security discussion about our proposed key distribution scheme will be shown. Then in Section IV, Investigation of Security we will compare our scheme with case study. Finally, we will conclude the paper in (H. Khurana *et al*, 2010) Section V.

3. The Proposed Secure Key Distribution Scheme



$$s \longleftarrow R_k$$
$$r \longleftarrow R_k$$
$$\varepsilon = \mathcal{E}_{k_m}(f_{k_s}(ID_m))$$
$$\beta = H_2(f_{k_s}(ID_m), r, s, 0)$$
$$\delta = H_2(f_{k_s}(ID_m), s, 1)$$

Fig.1 Secure Communication Message flow

3.1 System Components

According to the visionary model introduced by National Institute of Standard Technology (P. McDaniel *et al*, 2009), we consider four types of defined components similar to the principals depict in including trust anchors, data collectors and data aggregators. In this paper, we focus on the secure communication between the consumer and the producer, that is, the smart meter and the service provider in the smart grid. A trusted third party is used in our communication model.

1) Smart meter: A smart meter works as a collector collecting data and communicating with its service provider. It is an electronic device that uses two-way communication. It records utilization in intervals of an hour or less (S. William *et al*, 2011) and sends it regularly to the utility for observe and billing purposes. In other words, it is an enhanced home energy monitor able to gather data for remote reporting in short intervals. The most symbolic advantage is the ability of real-time monitoring including features such as power outage warning and power quality monitoring. Obviously, the smart meter plays an important role and has a high hardware requirement. To make communication secure, it contains a crypto processor having the ability of operating cryptographic computations. Currently, most of the smart meters are able to be connected with a computer through a serial cable, as a result, it leaves vulnerabilities for an attacker to manipulate the smart meter. It is very inconvenient to setup a smart meter as high as 16 feet even though this height can prevent the meter from being physically stolen (D Wu *et al*, 2011). Therefore, in our model, a secret key is stored in the tamper resistant memory of a smart meter. The key is used to interact with the trust anchor and gain a shared key between the meter self and the service provider. Without this secret key, the attacker could not impersonate the meter.

2) Service provider: It is the data aggregate supervisor the electric flows and send the on-time electric information to the user or smart meter. Upon receiving a message from a smart meter, it needs to authenticate the smart meter to response the demand. After obtaining the response, in the form of reply the smart meter needs to authenticate the provider as well. In our model, each service provider should also have a secret key which is created by Identity of Service Provider.

3) Trusted third party: The trust anchor is a trusted third party and manages the key distribution for the smart meter and the service provider. It manages the secret key of the smart meter and the service provider. To generate a secret key for one component with identity, the TA uses its master key and a one-way hash function (e.g., SHA-256) to compute the secret key for each user in this way where is a large prime. Therefore, Trust Anchor only needs to store its master key and the hash function for computation of the secret key of each component in the smart grid will show that set up this server as a Lightweight Directory Access Protocol

server since retrieving data from the server is more than write in our particular scheme for the smart grid.

These Three systems want to communicate securely with an help of secrete key A key management is a very important security issue in networks with an identity and algorithm for security.

3.2 Protocol working steps

In this implementation, Alice (sender) who is Smart Meter wants to communicate with Bob (receiver) who is Service Provider through Trust Anchor. Therefore, it is essential to agree on a specific basis to be able to do so. In the proposed protocol, a classical public key cryptography is used to send the basis which allows the two communicating party's. Secure Key Distribution scheme is initiated by a smart meter and the meter wants to establish a session key with another principle the service provider. After the two principles accept, the protocol assigns as the shared key for the two principles. In fact, Secure Key Distribution Scheme can be started by a service provider as well. Notice that Secure Key Distribution Scheme also can be applied for the communication between a service provider and an operation center with a trusted third party in the middle of them. Below is the description of Secure Key Distribution Scheme

Steps:

1) Smart Meter M sends own ID_m and Trust Anchor ID_s to initiates session which is first step of protocol initialization.

2) Smart Meter M sets $r \leftarrow R_k$ where r is a random number sends (R, ID_m) to a service provider.

3) Trust Anchor receives $(ID_m, ID_s)$from smart Meter M and computes $\varepsilon = \varepsilon_{k_m}(f_{k_s}(ID_m))$ where k_s is the service provider's secret key which is generated by one way hash function applied on Service Provider ID and k_m is the secret key of the smart meter M generated by one way hash function takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output applied on Smart meter ID.

4) Service provider obtains r , computes $(f_{k_s}(ID_m))$, sets $s \leftarrow R_k$ accepts setting , computes beta parameter $\beta = H_2((f_{k_s}(ID_m), s, ID_m, ID_s)$ and sends (S, β) to M and computes $\omega = .H_2((f_{k_s}(ID_m), s, ID_m, ID_s)$

5) Smart meter receives (S, β) and checks $\beta = H_2(k, r, s, 0)$ if above verification goes through successfully, then Smart meter accepts setting $\omega = .H_2((f_{k_s}(ID_m), s, ID_m, ID_s)$, otherwise rejects So from above Executing steps Secure Key Distribution protocol is communicated on the base of secrete key.

Table 1 Experimental procedure parameters in SKDP

Main Components	Required Keywords
Trust Anchor	k_s, k_m, ε
Smart Meter	$(S, \beta), \omega$
Service Provider	r, ω, β

Test cases	Description	Test status
Verification of selecting Identity Information	The Identity should be generated and along with random number	PASS. It should be properly Select in the correct format of Identity String.
Verification of key provided	The key will be given to Encrypt the messages.	PASS. If the Message is Encrypted to given a key else The encryption will not be Performed.
Verification of encryption	The selected document Should be encrypted by using Cryptography algorithm.	PASS. If the message is Encrypted properly and if it Has a correct format. Else The encryption will not be Performed.
Verification key	The user has to give the key To decryption.	PASS. If the user given the key it will be decrypted else it cannot decrypted.

3.3 Analysis of the Proposed Protocol

The proposed protocol takes advantage of the current public key cryptography protocols and the physical features of the quantum channels. It provides authentication and confidentiality. The main purpose of the proposed protocol is to ensure that a session key is delivered to the communicating parties in a secure manner.

1 .Precaution of the secret key: First, in our new key distribution scheme, Trust Anchor maintains the system secret x and p, whereas the user knows nothing about them. Second, the secret key for the smart meter is stored in the smart device's tamper-resistant memory, so we assume that the attacker is unable to read this sensitive information. In fact, even for an adversary who knows the user's secret key, it is still difficult for an attacker to recalculate p or x .

2. Man-in-the-middle-attack: In the man-in-the-middle attack, the attacker could intercept the messages between Trust Anchor and smart meter or between smart meter and service provider in proposed scheme, and then attacker replaces the old message with attacker's own message. In our scheme, may replace

the identities with's own identity. For example, to initiate this protocol, the attacker can send (ID_m, ID_a) to Trust Anchor where ID_a is attacker identity which is replaced from Service Provider Identity as in Proposed Work so that attacker should work like as service provider in secure key protocol while smart meter communicates with attacker it assumes that he will be communicates with service provider.

Conclusions

1) The envisioned smart grid will require a robust cryptosystem to meet the demands of Confidentiality, integrity, and availability. Conventional wisdom holds that Public Key Infrastructure is the good.
2) The requirements on key management for smart grid. A key management scheme is proposed for its use in smart grid and it meets these requirements. The security of the proposed scheme is built on the foundation of a public key infrastructure.
3) A new secure key distribution scheme for the smart grid with high efficiency as well as high security. Particularly for the trust anchor which is set up in a third-party environment, it can work as lightweight as a LDAP server.
4) we show that our proposed protocol is secure against man-in-the-middle so forth. Compared to the traditional public key infrastructure.
5) According to smart grid the three components in system lastly Smart meter, Trust Anchor, Service Provider communicates securely with the help of key distribution

References

S. William and W. Stallings (2011), Cryptography and Network Security, 6th ed. Pearson Education.

P. McDaniel and S. McLaughlin, (2009) Security and privacy challenges in the smart grid, *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77.

D. Wu and C. Zhou, (2011) Fault-tolerant and scalable key management for smart grid, *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 371–378.

A. R. Metke and R. L. Ekl,(2010) Smart grid security technology, *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107.

V. Shoup,(1996) Session key distribution using smart cadrs, in *Proc. EUROCRYPT 96*, pp. 321–331.

H. Khurana,M.Hadley, N. Lu, andD. A. Frincke,(2010) Smart grid security issues, *IEEE Security Privacy*, vol. 8, no. 1, pp. 71–85.

J. Naruchitparames, M. H. Gunes, and C. Y.Evrenosoglu,(2011) Secure communications in the smart grid, in *Proc. IEEE Consumer Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, pp. 1171–1175.

X. Cao, W. Kou, Y. Yu, R. Sun,(2008) Identity-based authentication key agreement protocols without bilinear pairings, IEICE Transaction on Fundamentals ,E91–A(12):3833–3836.

Z. Cheng, M. Nistazakis, R. Comley, L. Vasiu,(2005) On the in distinguishability-based security model of key agreement protocols-simple cases, Cryptology ePrint Archieve, Report 2005/129.

H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, (2010) Design principles for power grid cyber-infrastructure authentication protocols, in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, Honolulu, HI, Jan. 2010, pp. 1–10.

C. H. Bennett, G. Brassard *et al*.(1984.), "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, no. 0. New York.