International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.17-24
http://dx.doi.org/10.14257/ijsia.2014.8.6.02

P_PAKA: Privacy Preserving Authenticated Key Agreement Protocol in Smart Grid

Hyunsung Kim

Dept. of Cyber Security, Kyungil University
kim@kiu.ac.kr

Abstract

The current power grid is changing into a network of interoperating intelligent devices to form a smart grid. One of the technologies enabled by the bi-directional communication of the grid is demand response (DR), which allows regulation of energy loads by efficiently shifting consumer power demand of non-critical appliances from on-peak to off-peak with price incentives for compliance. However, security and privacy of communications between entities are the major constraining factors to the adoption of smart grid applications. Therefore, this paper proposes a privacy preserving authenticated key agreement protocol (P_PAKA) in smart grid that addresses the privacy issues for DR communications. We demonstrate the provision of desirable security features and requirements of confidentiality, integrity and availability in DR with unlinkability.

Keywords: *We would like to encourage you to list your keywords in this section*

1. Introduction

Smart grid technologies rely on a wide collection of user data including power usage, which can reveal personal information such as user's location, behavior, the amount of energy consumed, and the type of devices they own [1-2]. By increasing the amount of collected consumer information, new forms of attacks propagate. So, proper authentication, authorization and privacy mechanism form the main security solutions for consumer protection. As privacy of terminal customers and smart metering networks is important to the eventual acceptance of the smart grid by the public, a solution to the problem of its threats would be vital. In strict sense, the customers may not even want the third party utility service providers know their specific identity throughout the normal transactions involving advanced metering infrastructure (AMI) [3]. Therefore, confidentiality and integrality can deal with the perceived cyber-threats by employing encryption and privacy preserving authentication mechanisms. To ensure secure network communication the key must be securely derived and managed in AMI and DR systems which entail the necessity of employing secure authentication and key management mechanisms [4-7]. Especially for example, for the AMI system, best practices such as, confidentiality for privacy protection, and integrity for firmware updates forms the basis of secure communication authentication of the meter to the collector, AMI and DR system. In smart grid architecture, there are several relay gateways and higher levels communications from home area network (HAN) to utilities (UT) or service provider (SP), but in this protocol presentation we just consider the communication between smart appliances (SA) and smart meter (SM), SM and gateway (GW) and then communication between GW and SP based on the trust-ship each party builds first with UT. We assume that SM and GW communicate securely using an

ISSN: 1738-9976 IJSIA

established symmetric key but GW and SP communication requires security measures. SP can be visualized as a data aggregator within the WAN responsible for monitoring electricity flows and send the on-time electric information to the user or smart meter.

This paper proposes a privacy-preserving authenticated key agreement protocol, named as P_PAKA, for service provision in smart grid communication. Particularly P_PAKA focuses on securing the HAN and service provider sub-system communications. In due regards to smart grid communication requirements the main contribution of this paper are (a) privacy-preserving authentication protocol for HAN and service providers communications with non-repudiation (b) certificate less authentication procedure which precludes the heavy management load of public key infrastructure (PKI) such as the scalability of the infrastructure and certificate management and (c) efficient authentication protocol which is pairing-free therefore suitable for resource constrained smart grid field devices. Due to efficiency factor P_PAKA can achieves low latency smart grid requirement since it has low computational overhead.

2. Mathematical Preliminaries

This section gives an introduction of the fundamental mathematical backgrounds of the proposed protocol [8-12].

2.1. Computational Diffie-Hellman Problem (CDH)

Given parameter (g, g^x, g^y) in a cyclic group G of an order q, where $x, y \in Z_q^*$, the CDH is the problem of finding $g^z = g^{xy} \in G$ [8].

2.2. Hash Chain Function

We first introduce the concept of one way hash function which is the fundamental of hash chain function and forms the basis for the security of P_PAKA [9]. A hash function $h()$ takes a random string of arbitrary length as input and outputs a string of arbitrary length. A one way hash function satisfies the following properties: (1) given x it is easy to compute x it is easy to compute y such that $y = h(x)$; (2) given y it is computationally infeasible to compute x such that $y = h(x)$. The privacy preserving features in the proposed protocol are based on one way hash function in the form of a hash chain function. A back hash chain is formed by recursively hashing a random number n_1 and line up the output in a sequence, $N_1, N_2, \ldots, N_n$ using hash operation in reverse order such as:

$$N_i = h(N_{i+1}), \text{ for } i = n-1, n-2, \ldots, 0.$$

Thus, GW chooses a random number n_1 and produce the a hash chain $h^{(1)}(n_1)$, $h^{(2)}(n_1)$, …, $h^{(n)}(n_1)$ where n is the total number of operations and $h^{(i)}(n_1) = h(h^{(i-1)}(n_1))$ for $i = 1,2, \ldots, n$ to carry out authentication procedure with SP. Firstly, GW share verifiable $N_1 = h^{n+1}(n_1)$ with SP through the help of a trusted party UT. Thereafter, GW can securely send SP a subsequent hash value in the hash chain which is used in the derivation of a shared secret. SP can verify the authenticity of the received random number by carrying out:

$$N_i ? = \underbrace{h(h(h \ldots h}_{i}(h(n_1) \ldots)))$$

Notice SP is able to verify by using a pre-shared value in the recursive sequence due to the one-way property. At the end of the message transmission, GW is able to authenticate itself anonymously with unlinkability and non-repudiation throughout the whole sequence of generated random numbers. If the finite number of random numbers is exhausted GW generates a fresh sequence of hash chain and repeats the processes of sharing the seed of the hash chain values with SP securely through UT. On the other hand GW know only SP has the subsequent seed values. If the procedure is successful the parties mutually authenticate each other. The technique of backward hash chain function in authentication process is presented in [10-12].

3. Privacy Preserving Authenticated Key Agreement Protocol

The proposed P_PAKA takes four phases for key agreement, but in the first authentication it will take five phases which are: Set-up, Registration, Service subscription, Authentication phases. P_PAKA is well designed for AMI applications whereby communications originate from the customer side to the SP.

3.1. Set-up

The UT as the root entity produces system parameters as follows:

(i) UT generates two primes p and q such that $g = h^{(p-1)/q} \bmod p$, where $h \epsilon [1, p-1]$.

(ii) Afterwards, UT chooses two private keys, x and x_v and then compute their corresponding public keys $v = g^x$ and $y_v = g^{x_v}$ respectively.

(iii) UT sets x as the master secret key (*Msk*) and shares the private key x_v, K_{UT-SP} and y_v with an SP during its registration.

Then publishes *params*= $\{p, q, g, h(), H()\}$ as the system public parameters.

3.2. Registration

Both GW and SP register with UT to obtain private keys. In registration GW seeks to obtain a pseudonym from UT to be used to conceal its actual identity on the network. Whilst SP obtains a symmetric key shared with UT to bind confidentiality of their transactions. Below is how the procedure for GW registration goes:

(i) GW submits identification information, ID_{GW}, in a secure manner.

(ii) UT computes a proxy key pair $K = g^k$ and $\sigma = x + kh(K)$ where $k \epsilon Z_q^*$ for each GW.

(iii) UT stores (σ, K) while (σ, K, y_v) are stored in each GW.

In a similar manner, SP also registers with UT in order to get service provision permission as follows:

(iv) SP submits its identification details and a description of services it wishes to provide (ID_{SP},*Service*) to UT.

(v) UT checks the legitimacy of SP before granting services warrant.

(vi) If SP is acceptable, UT registers the services offered by SP on its portal and then sends the private key x_v, the secret key K_{UT-SP}, and y_v to SP.

3.3. GW Service Subscription

After proper registration, GW can now subscribe preferred services for a particular SP published on UT's portal. GW's service subscription steps proceeds as follows:

(i) Whenever GW want to subscribe to SP's services publishes on UT's portal, it chooses a random number $n_1 \epsilon Z_q^*$ as the seed of a hash chain function and computes the hash chain $h^{(i)}(n_1) = h(h^{(i-1)}(n_1))$ for $i = 1,2, \ldots, n$. Sets $N_1 = h^{n+1}(n_1)$, then computes $T_1 = H(K||ID_{UT}||N_1||SP)$, $T_2 = E_\sigma(ID_{GW}, ID_{UT}, ID_{SP}, N_1, K)$ and sends subscription request $\{T_1, T_2, K\}$ to UT.

(ii) After receiving the message, UT checks corresponding secret key σ to the received pseudonym K and uses it to decrypt T_2. Upon decryption, then UT checks if $T_1 = ? H(K||ID_{UT}||N_1||ID_{SP})$ holds.

(iii) If the verification holds, UT chooses a random number $n_2 \epsilon Z_q^*$ and sends the warrant of service subscription to SP by sending $Enc_{K_{UT-SP}}(T_3||l||n_2||K||T_4||ID_{UT})$ where $T_3 = Enc_\sigma(N_1||n_2||ID_{SP})$, $T_4 = H(K||l||ID_{SP})$ where $N_1 = l$.

(iv) SP gets $T_3||l||n_2||C_1||K||T_4||ID_{UT}$ after decryption of the received message from UT with the pre-shared symmetric key K_{UT-SP}. First SP check the integrity of K and l by using T_4 and if the checking holds proceeds with the process, otherwise it aborts the session.

(v) SP select a random number $n_3 \epsilon Z_q^*$, compute $C_1 = h(N_1||n_2||n_3||ID_{SP}||ID_{GW})$ and then sends $\{T_3, C_1, n_3\}$ to GW and sets a token for subscription $SK = C_1$. Then SP includes (K, l, C_1) to the list of its subscribers in its directory for verification of permission to access services for subquent communications involving the owner of the credentials

From the received message, GW verifies C_1 after decrypting T_3. If the verification holds, GW sets $SK = h(N_1||n_2||n_3||ID_{SP}||ID_{GW})$ as a subscription token to use later to obtain services.

3.4. Authentication Phase

Whenever GW wishes to communicate with SP securely, it presents the token and anonymous identification information while still supporting non-repudiation on SP's view point. GW carries out the following authentication procedure together by utilizing the backward hash chin function.

(i) GW retrieves the pre-computed backward chain value in the sequence of random numbers, say, N_2 such that $N_1 = h(N_2)$ and computes $r_1 = g^t$, $r_2 = H(y_v{}^t) \oplus (K, C_1, N_2)$. Then, GW sends $\{r_1, r_2\}$ to SP.

(ii) SP uses x_v to extract K, C_1 and N_2 by computing $H(r_1{}^{x_v}) \oplus r_2$. Then SP cross-checks the token C_1 against the pseudo-identity K. If the checking is successful SP proceeds to verify whether the computed value $h(N_2) = h(h^n(n_1))$ equals the stored value in its database $l = h^{n+1}(n_1)$.

(iii) If the authentication holds SP updates $l = N_2$ and then computes the session key $C_2 = h(l, C_1)$ and finally updates counter. SP sends a confirmation message, $C_2{}' = h(C_2, ID_{SP}, K)$ to GW.

(iv) GW checks if $C_2{}' = h(C_2, ID_{SP}, K)$ and agree on the session key value $C_2 = h(N_2, C_1)$ otherwise aborts the session. In general, both GW and SP use $SK = C_{i+1}$ as the current session key and update counter to $i = i + 1$ for $i \leq n$.

4. Security Analysis

In this section, we show how P_PAKA satisfies the security requirements suitable for smart grid communications. The focus is to secure out-going transmission from HAN to SP and vice-versa. Once outgoing messages are secured it is inferred that AMI and other real time communication to the SP are secure. In a similar manner if incoming communication are secured, it implies that DR and other control commands messages from SP and operations domain are secure hence achieving secure smart grid at large.

4.1. Unlinkability/Anonymity

P_PAKA achieves anonymous authentication of the GW to SP without disclosure of user's real identity, ID_{GW}. This is achieved by sending the authentic value K encrypted during subscription phase from GW to UT and $\{r_1, r_2\}$ from GW to SP during authentication phase. There is no way an attacker can discover the user's real identity because no user identification material is transmitted in plain. Although the component $r_2 = H(y_v{}^t) \oplus (K, C_1, N_2)$ carries the pseudonym K for GW but still more it is not accessible to unintended parties or an eavesdropper on the communication. Therefore the protocol provides user anonymity because GW uses a pseudonym K. The kind of anonymity employed is conditional anonymity, such that in case of dispute SP can engage UT to revoke the actual identity of GW. Further unlinkability is provided because the pseudonym K is protected from the preying eyes of an adversary and therefore cannot be related to a particular user GW by anyone other than SP. So, personal privacy is guarded against an eavesdropper and SP. This means the session key derived after authentication ensures privacy of end user metering data information like metering data or any encrypted messages. Even if the attacker just attempt to trace whether a marked legal user GW has transacted with SP, the attacker will not succeed because the real identity is never disclosed and the login authentication message $\{r_1, r_2\}$ is dynamic due to the random number $t \epsilon Z_q{}^*$ in r_1 and r_1. Thus, it is impossible to link two different instances of the authenticated messages into the same user, GW, even if both messages are in the hands of an adversary.

4.2. Impersonation Attack

An attacker may attempt to use a bogus GW to impersonate the real GW that the attacker has access to, in order to authenticate to the remote service provider or vice versa. As much as the attacker has no knowledge of the GW due to anonymity and unlinkability properties, the attacker cannot manage to impersonate the user with a malicious GW to the service provider. Even from the transmitted messages, $\{r_1, r_2\}$ and $\{T_3, C_1, n_3\}$ relayed between SP and GW, the attacker cannot modified them to pass authentication because he/she will need to have the secret value σ to access K in order to impersonate either GW or SP to pass the counterpart's verification. This attack is difficult to materialize because the real identity of the user is still concealed to all players in the system except UT.

4.3. Replay Attack

An attacker may wish to initialize a replay attack from eavesdropped data packets of an authenticated communication between the GW and SP and retransmit them at a later time as if it comes from the real GW. This attack is thwarted in P_PAKA because the authenticated token $SK = \mathrm{h}(N_1||n_2||n_3||\sigma)$ for subscription phase contains random

numbers N_1, n_2 and n_3 meant to be used once, so there is no way an attacker can devise a replay of any message encrypted with the session key. In the same way the session key $SK = h(l, C_i)$ for regular session authentication phases is unique per session and is updated after any successful authentication procedure. So its arguable P_PAKA resists against the replay attack.

4.4. DoS Attack

In P_PAKA , the communications between GW and SP do not require a synchronous update. Hence resist attacks that result into desynchronization like reflection attack or replay attack. That means the legal parties, either GW or SP, will not be prevented from communicating by an adversary at any instance. At the end, P_PAKA offers resistance to DoS, thereby satisfying a desirable communication requirement for the DR communication in smart grid. This ensures delivery of quality and reliable electricity management services.

4.5. Man-in-the Middle Attack

In man-in-the-middle attack, an adversary eavesdrops and intercepts the communication between or among communicating legal parties and relays authentic messages to the victims to make them that believe they are communicating confidentially. Thus, the adversary controls the whole communication sessions without knowledge of the intended parties. However this attempt though cannot succeed in the proposed protocol because no attacker can manage to initiate the fabrication of a session key that seems acceptable before GW and SP. Since to achieve this attack, the adversary must find a means of sending verifiable components K, C_1, N_2 in order to pretend as GW to SP. Obviously, there is no other way of forging N_2 without knowledge of the random seed of the hash chain function. Furthermore, the extraction of N_2 means the ability to solve the computation of $r_2 \oplus H(g^{x_v t})$, which is a CDH problem that can be solved by GW and SP only. Therefore the attacker will not succeed and besides the values K is not sent in plain, thus the attacker will not know the pseudonym of a targeted GW. Conclusively the proposed protocol is resilient against impersonation attack.

4.6. Mutual Authentication

In P_PAKA, both end point the origin and the destination of a transmitted message authentication and verify the authenticity of the counterpart, thereby providing mutual authentication. Before GW and SP can communicate securely they first share a random number by the help of a trusted authority UT. So based on a pre-shared random number $l = N_1$ the parties transmit messages authentic and verifiable only between themselves. For instance, when GW sends login message $\{r_1, r_2\}$ to SP it is formed in a way that only SP with the knowledge of the private key can extract the fresh random number N_2 by using the private key x_v by computing $H(y_v{}^t) \oplus (K, C_1, N_2) \oplus H(g^{x_v t})$. Having extracted N_{i+1}, SP verifies the relationship $N_i = h(N_{i+1})$ and the pseudonym K before computing a session key $C_{i+1} = h(l, C_i)$. If the verification holds then the pseudonym is authenticated. On the other hand GW authenticates an SP by checking the received confirmation message $C_2{}' ?= h(C_2, ID_{SP}, K)$ from SP. GW's trust that it is communicating with an unintended party is based on the assumption that computing $H(y_v{}^t) \oplus (K, C_1, N_2) \oplus H(g^{x_v t})$ without knowledge of SP's private key involves

solving the CDH problem $g^{x_v t}$ which is infeasible by an attacker. At the end GW and SP mutually authenticate each other.

4.7. Forward Secrecy

P_PAKA provides forward secrecy for SP. That is even if the long term private key x_v is compromised still more, future session keys $SK = C_i$ will not be compromised. This is so because the session key includes a securely pre-shared random number l such that $SK = h(l, C_i)$. Even it is possible to extract C_i from the message $\{r_1, r_2\}$ by computing $H(y_v{}^t) \oplus (K, C_1, N_2) \oplus H(g^{x_v t})$ with the knowledge of the private key x_v the adversary does not know the pre-shared value l. The only way an unintended party can know the pre-shared random number is by decrypting the message $Enc_{K_{UT-SP}}(T_3||l||n_2||K||T_4||ID_{UT})$ from UT to SP sent during service subscription. Unless the adversary acquires both the private key x_v and the symmetric key K_{UT-SP} the attack on subsequent session keys cannot be accomplished. This property upholds the confidentiality and integrity of the communication.

5. Conclusion

This paper proposed P_PAKA protocol in smart grid. DR function allows utility as well as consumer to make decisions on electricity management enabled by two-way communication of electricity and information in the system. It is necessary that communications between the parties provide rapid response with a goal of maintaining load balance. Although smart grid has and promises many benefits, security vulnerabilities and potential privacy threats draw back full adoption. Therefore securing the system by cryptographic and non-cryptographic mechanisms is part of important implementation effort to establish customer confidence. In this regard, the objective of this paper is addressing the smart grid privacy of DR communications with low computational overhead, which also provide unlinkability, anonymity, impersonation attack resilience, replay attack resilience, DoS resilience and man-in-the-middle attack resilience. Further, it provides security enhancements of mutual authentication and forward secrecy. These properties ensure the credibility of the system communications.

Acknowledgements

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575).

References

[1] W. Wang and Z. Lu, “Cyber security in the Smart Grid: Survey and challenges”, Journal of Computer Networks, vol. 57, **(2013)**, pp. 1344–1371.
[2] Y. Yan, Y. Qian, H. Sharif and D. Tipper, “A survey on smart grid communication infrastructures: Motivations, requirements and challenges”, IEEE Communications Surveys & Tutorials, vol. 15, no. 1 **(2013)**, pp. 5–20.
[3] A. A Cardenas and R. S Naini, “Security and Privacy in the Smart Grid”, Handbook on Securing Cyber-Physical Critical Infrastructure, DOI: 10.1016/B978-0-12-415815-3.00025-X 637, **(2011)**.
[4] D. Wu and C. Zhou, “Fault-tolerant and scalable key management for smart grid”, IEEE Transactions on Smart Grid, vol. 2, no. 2, **(2011)**, pp. 371–378.
[5] J. Xia and Y. Wang, “Secure Key Distribution for the Smart Grid”, IEEE Transactions on Smart Grid, vol. 3, no. 3, **(2012)**, pp. 1437-1443.

[6] N. Liu, J. Chen, L. Zhu, J. Zhang and Y. He, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid", IEEE Transactions on Industrial Electronics, vol. 60, no. 10, **(2013)**, pp. 4746-4756.
[7] P. Deng and L. Yang, "A secure and privacy-preserving communication scheme for Advanced Metering Infrastructure", Proc. of 2012 IEEE PES Innovative Smart Grid Technologies, **(2012)**, pp. 1-5.
[8] J. Hoffstein, J. Pipher and J. H. Silverman, "An introduction to mathematical cryptography, Springer, **(2008)**.
[9] K. Q. Nguyen, Y. Mu and V. Varadharajan, "Digital coins based on hash chain", Proc. of National Information Systems Security Conference, **(1997)**.
[10] T. F. Lee, S. H. Chang, T. Hwang and S. K. Chong, "Enhanced delegation-based authentication protocol for PCSs", IEEE Transactions on Wireless Communications, vol. 8, no. 5, **(2009)**, pp. 2166–2171.
[11] W. B. Lee and C. K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems", IEEE Transactions on Wireless Communications, vol. 4, no. 1, **(2005)**, pp. 57–64.
[12] J. L Tsai, N. W Lo and T. C Wu, "Secure Delegation-Based Authentication Protocol for Wireless Roaming Service", IEEE Communications Letters, vol. 16, no. 7, **(2012)**, pp. 1100-1102.

Author

Hyunsung Kim, he is a professor at the Department of Cyber Security, Kyungil University, Korea from 2012. He received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.

