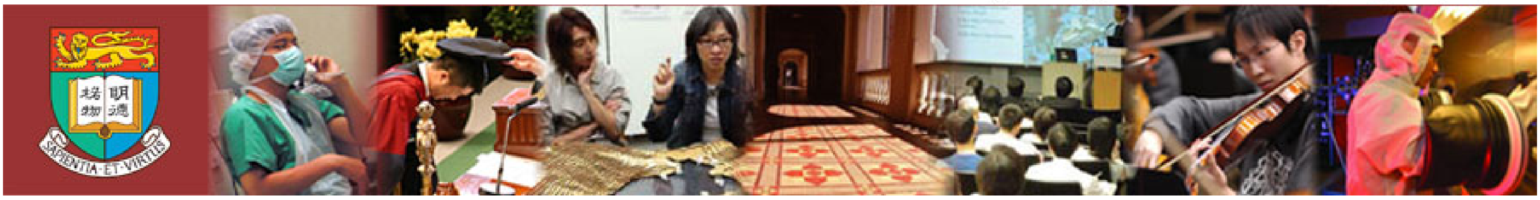

PASS: Privacy-preserving Authentication Scheme for Smart Grid Network

T.W. Chim, S.M. Yiu and Lucas C.K. Hui
Department of Computer Science
The University of Hong Kong
Email: {twchim, smyiu, hui}@cs.hku.hk

Victor O.K. Li
Department of Electrical and Electronic Engineering
The University of Hong Kong
Email: vli@eee.hku.hk

***Abstract*—A smart grid power system is capable of adjusting the amount of electricity generated based on real-time requests from the smart meters of customers, thus avoiding excess electricity generation and facilitating reliable and effective transmission of electricity. To ensure that requests are sent from a valid user, all request messages must be authenticated. On the other hand, by analyzing the electricity usage pattern of a customer, the daily habit of the customer, such as when he is away, may be revealed. Thus, a proper privacy preserving mechanism has to be adopted. This paper attempts to develop a scheme to address these two seemingly contradicting requirements efficiently. By using a tamper-resistant device at the smart appliance and pseudo identities, we derive a privacy preserving authentication scheme to solve the problem. The authentication process is made very efficient by means of Hash-based Message Authentication Code (HMAC). Through simulation, we show that with our scheme, the transmission and signature verification delay induced are very small and the message overhead is only 20 bytes per request message. With our efficient verification process, even under attack, the substation can effectively drop all attack messages, allowing 6 times more valid messages to reach the control center when compared to the case without any verification. Thus our scheme is both efficient and effective.**

***Index Terms*—Smart grid network, authentication, privacy preserving, pseudo identity, tamper-resistant device**

I. Introduction

A smart grid is considered as the next generation power supply network which facilitates reliable and effective transmission of electricity from power generators to household electric appliances. In this network, the amount of electricity generated can be adjusted according to the real-time demand of consumers. This not only ensures that consumer demands are satisfied but also avoids excess electricity generation. The latter can help increase the profit of the power operators and protect the environment. In the future, a smart grid network may also facilitate a consumer to sell unused electricity back to the power operator.

As suggested by [1], a smart grid network is roughly divided into three layers: (1) power operator; (2) substations; and (3) smart meter (usually one per household) and smart appliances of customers. Figure 1 shows a simplified architecture of a smart grid network. Each customer premises is assumed to have a smart meter installed. The smart appliances in the household will communicate with the smart meter which will then communicate with the substation via existing wireless or wired networks (e.g. Internet through the routers in the premises). The substations will collect real-time demand and usage information from smart meters and forward the information to the power generator systems for further analysis and processing. The power generators and the substations communicate through the Supervisory Control and Data Acquisition (SCADA) system [2].

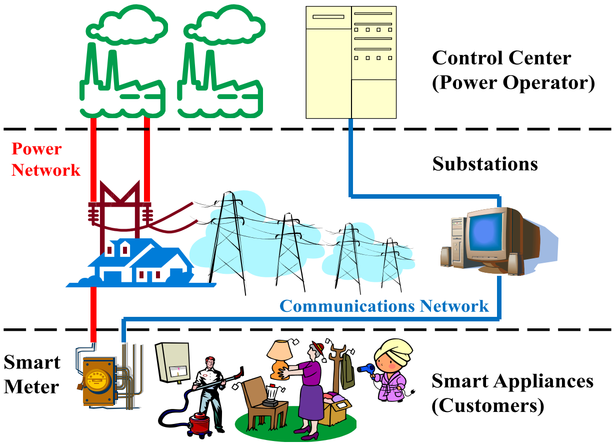

Fig. 1. Simplified Architecture of Smart Grid Network

Unlike the Kwh meters in the traditional power network, the smart meters will push information of the appliances to the substations periodically. In this paper, we focus on two major security issues of the communication between the substations and the smart meters.

Information flow from individual electric appliances to the substations (and then to the power generators) has great impact on the reliability of power supply and is related to the charges for the customers. Security issues in a smart grid system must not be overlooked. In particular, sender authentication and user privacy preservation are two major concerns [3].

Since the information sent by individual appliances determines the amount of electricity a generator has to generate, a proper authentication scheme should be imposed to ensure that the identity of the sender can be confirmed. On the other hand, unlike traditional Kwh meters which only record the cumulative amount of electricity used, the smart meters transmit real-time information of individual appliances to the substations.

978-1-4577-1702-4/11/$26.00 ©2011 IEEE

As a result, electricity usage patterns of the consumer will easily be traced and leaked. Such privacy leakage can be used to reveal the daily habits of the consumer such as when a consumer is not at home. This privacy preservation issue has been raised in [3], [4]. A proper privacy preserving mechanism has to be adopted.

The design of security schemes in a smart grid system to tackle the above issues is not trivial and subject to the following challenges. First of all, most data communications in smart grid network can be considered as critical. Any delay may result in the consumer experiencing electricity interruption. According to [5], the power generator system only has a few seconds to receive data from substations in each period. Any security schemes added to the system should be efficient in terms of time complexity. On the other hand, while the identity of a sender needs to be authenticated, we have to preserve the privacy of the consumers, and we do not want a substation to be able to analyze the exact amount of electricity needed by each appliance. Thus, techniques to enable a substation to process the information without knowing their actual contents, and to prevent linking the information to the users are required.

In this paper, we utilize the hierarchical structure of a smart grid and propose a novel tamper-resistant-device-based Privacy-preserving Authentication Scheme for Smart grid network (PASS). Recall that we only focus on the substation-to-consumer subsystem. Our scheme has the following security features:

1) Substations: which are physically more secure from being attacked, are responsible for basic authentication of messages sent by smart appliances on their way to the control center. This can help to ensure the availability of the power system.

2) Household smart appliances: which are more vulnerable to attacks, are made more secure by connecting them to tamper-resistant devices. It is a general assumption that keys stored on them are difficult to be cracked. In this paper, since smart appliance and tamper-proof device actually refer to the same electric device, we will use these two terms interchangeably.

3) The real identity of any smart appliance and the amount of electricity required by it from time to time can only be known by the control center. We make this possible using the concept of pseudo identity.

The rest of the paper is organized as follows. Related work is reviewed in Section II. The system model and the problem statement are included in Section III. Some preliminaries are given in Section IV. Our schemes are presented in Section V. The analysis and evalution of our schemes are given in Sections VI and VII. Finally, Section VIII concludes the paper.

II. Related Work

The smart grid project was initiated by the European Union in 2003 [6]. At around the same time, the IntelliGrid project [7] was started by the Electric Power Research Institute of the USA. The US DOE started the Grid 2030 project [8]. Under the Energy Independence and Security Act of 2007, the National Institute of Standards and Technology (NIST) is responsible for coordinating the development of a framework for information management to achieve interoperability of smart grid devices. In 2010, NIST released a report [5] which describes the potential components of a smart grid. Some security issues (which they define as cyber security) are also discussed.

A recent work [9] elaborates on the importance of a smart grid especially with the consideration of renewable energy resources. A new control model known as risk-limiting dispatch is described. Some new requirements of the communication architecture and potential security problems are identified. As such, there is an urgent need to establish protocols and standards for the smart grid.

In terms of security, the major issues are discussed in details in [3] and [4]. For the generator-to-substation communication, some security measures are already in place in the extended version of SCADA [10]. For the substation-to-appliance communication, sender authentication and user privacy preservation are considered as the two major concerns as discussed earlier. However, not much research has been done in this aspect yet.

III. System Model and Security Requirements

In this section, we discuss our assumptions and security requirements in details.

A. System model and assumptions

Recall that we consider a smart grid network to consist of three basic layers - power generators, substations, and smart meters and smart appliances. It can be easily observed that these three layers have different physical security level assumptions.

1) The power generator system (or referred to as the control center) is assumed to be secure and fully trusted.

2) Substations are usually physically locked from outside access as it contains expensive electric devices such as transformers. They are relatively more difficult to be compromised by attackers. In this paper, we assume that they are secure.

3) Electric appliances (as well as smart meters) are more vulnerable to physical disturbance and compromise since they are located at customers' homes and the power operator has no way to keep an eye on them.

Also without loss of generality, we assume that servers at the control center and the substations have higher computational power.

B. Security requirements

We aim at designing an authentication scheme to validate request messages from smart appliances which are located at customers' homes while at the same time, preserve the customers' privacy (such as daily electricity usage pattern). The security requirements are summarized as follows:

1) Message authentication: The request message from any electric appliance has to be properly authenticated before they are forwarded to and processed by the control center. Also an attacker cannot impersonate any valid electric appliance to send out fake request messages.

2) Identity privacy: The real identity of any electric appliance should be kept anonymous from any third party to protect the privacy of the customer concerned. In this way, a third party should not be able to relate multiple messages sent by the same electric appliance or even by the same customer.

3) Request message confidentiality: The amount of electricity required by any electric appliance should be kept confidential from any third party to protect the privacy of the customer concerned. A third party should not be able to trace the daily electricity usage pattern (and thus the daily habit) of any customer by collecting electricity request messages from them.

4) Traceability: Though the real identity of and the amount of electricity required by an electric appliance cannot be revealed by a third party, the trusted control center should have the ability to obtain any appliance's real identity and their electricity usage. This is necessary for the actual electricity supply determination.

IV. Preliminaries

In this section, we explain the concepts of public-key encryption, digital signature and hash-based message authentication code.

A. Public-key encryption and digital signature

Public-key encryption is a function provided by the public key infrastructure (PKI) and is also known as asymmetric encryption. A trusted party assigns each user a pair of public key and private key. The public key can be known by everyone while the private key is kept secret. To securely send a message, the sender encrypts the message using the receiver's public key. The receiver can then obtain the message by decrypting using the corresponding private key. RSA [11] is a well-known algorithm for public-key encryption. Throughout this paper, we denote the process of encrypting plaintext M with public key PK to obtain ciphertext C as $C = ENC_{PK}(M)$. Similarly, we denote the process of decrypting ciphertext C with private key SK to obtain plaintext M as $M = DEC_{SK}(C)$.

Public-key digital signature is another function provided by the PKI and is a direct extension of public-key encryption. Using the private key assigned by a trusted party, one can generate a unique signature on a message. The receiver can then use the sender's public key to verify the validity of the signature. RSA is a well-known algorithm for computing digital signature. Throughout this paper, we denote the process of signing message M with private key SK to obtain signature σ as $\sigma = SIG_{SK}(M)$.

B. Hash-based Message Authentication Code (HMAC)

Hash-based Message Authentication Code (HMAC) is a specific construction for computing a message authentication code (MAC) using a cryptographic hash function in combination with a secret key. Both data integrity and authenticity of a message can be achieved using such a technique. Well-known hash functions such as SHA-1 [12] and MD5 [13] can be extended to produce an HMAC. Due to the property of hash functions, an HMAC value can be computed in a much shorter time than a traditional digital signature. Throughout this paper, we denote the HMAC value generated on message M using the secret key K as $HMAC_K(M)$.

V. Our Solution - PASS

This section presents our Privacy-preserving Authentication Scheme for Smart grid network (PASS) in details.

A. Preparation module

As discussed earlier, each smart appliance (located at customers' homes) is attached with a tamper-resistant device for generating pseudo identities and signatures on messages (details will be discussed in the next sub-section and these are the only functions that can be carried out by the device). The tamper-resistant device has a clock which runs on its own battery. Clocks on tamper-resistant devices are assumed to be roughly synchronized. A customer is given that device when he/she opens an account or registers a newly purchased smart appliance at the power operator.

The control center generates its public and private keys. We denote Pub_{cc} as its public key which is assumed to be preloaded into all tamper-resistant devices. Pri_{cc} is its private key (corresponding to Pub_{cc}) and is kept private.

Assume that the region controlled by substation ST_r is denoted by R_r. The control center first assigns ST_r an identity SID_r. It then generates an initial system key s_r and saves it into all tamper-resistant devices located in region R_r as well as the substation ST_r (for signature verification purpose; details will be discussed in the next sub-section). The control center stores $< SID_r, s_r >$ in its local database.

The control center assigns each smart appliance A_i a real identity RID_i which is securely preloaded into its tamper-resistant device. Besides, it also generates a pair of public and private keys, Pub_i and Pri_i respectively, and securely preloads them into the tamper-resistant device. The term "securely" means that RID_i cannot be known or modified by an unauthorized party easily. The control center stores $< RID_i, Pub_i >$ in its local database. Besides parameters, the tamper-resistant device also has two (and only these two) functions pre-loaded: 1) Generation of pseudo identity based on the smart appliance's real identity. The details will be discussed in Section V-B. 2) Generation of HMAC value on a given message using the regional system key. The details will be discussed in Section V-C.

B. Pseudo identity generation module

Now assume that the smart appliance A_i wants to request more electricity supply from the control center.

A_i's tamper resistant device first generates a pseudo identity PID_i as $PID_i = ENC_{Pub_{cc}}(RID_i||r)$ where $||$ represents a pre-defined form of concatenation and r is a per-session random nonce. When we look closer, $ENC_{Pub_{cc}}(RID_i||r))$

actually represents encrypting the concatenation of RID_i and r using the control center's public key. Note that r is necessary here so that two pseudo identities from the same smart appliance cannot be linked up easily by an eavesdropper.

C. Signing module

Assume that the amount of electricity requested is denoted as M_i. A_i's tamper-resistant device first extracts the current timestamp T_i from its clock and generates its signature on the request message M_i as $\sigma_i = HMAC_{s_r}(PID_i||ENC_{Pub_{cc}}(M_i)||T_i)$. Recall that s_r is the regional system key.

Finally, A_i sends $< PID_i, ENC_{Pub_{cc}}(M_i), T_i, \sigma_i >$ to the control center via the smart meter in the household and its regional substation.

D. Verification module

Without loss of generality, we assume that the substation which is in A_i's region is ST_r. Upon receiving the message $< PID_i', ENC_{Pub_{cc}}(M_i)', T_i', \sigma_i >$ from A_i, ST_r drops it if the timestamp T_i' is outdated (say much longer than the average transmission time concerned). This procedure can help minimize the impact of replay attack.

If the timestamp is not outdated, the substation ST_r verifies the signature by checking whether $HMAC_{s_r}(PID_i'||ENC_{Pub_{cc}}(M_i)'||T_i')$ is equal to σ_i. If not, the substation simply drops the message. If the signature is valid, it forwards the message to the control center.

The substation ST_r stores all pseudo identities, encrypted request messages together with HMAC signatures locally so that they can be transmitted to the control center in a batch at a later time for investigation purpose when an attack takes place.

E. Tracing module

Upon receiving the forwarded message from the substation ST_r, the control center first reveals A_i's real identity RID_i based on its pseudo identity PID_i. This can be done by decrypting $ENC_{Pub_{cc}}(RID_i||r))$ using its private key Pri_{cc} and then removing r from the end of the block $(RID_i||r)$.

After that, the control center arranges to update the current power supply rate to fulfill A_i's requirement accordingly.

VI. Security Analysis

We analyse our scheme with respect to the security requirements listed in Section III.

1) Message authentication: Before a smart appliance transmits a request message to the control center, it has to include an HMAC signature on the message using the regional system key. This regional system key is only known by the control center, the substation and all tamper-resistant devices within the region. Hence an outside attacker (who does not belong to the region or is not a registered smart appliance) does not know how to generate a valid HMAC signature. Thus our scheme is protected from outsider attacks.

2) Identity privacy: In all request messages sent by a smart appliance, pseudo identities instead of real identity is used. The pseudo identity PID_i of smart appliance A_i is defined as $ENC_{Pub_{cc}}(RID_i||r)$ where r is a per-session random nonce. Since RID_i is encrypted using the public key of the control center, no one except the control center can decrypt it. Also with the per-session random nonce r, two pseudo identities belonging to the same smart appliance cannot be related by an eavesdropper easily.

3) Request message confidentiality: The amount of electricity required by a smart appliance is encrypted using the public key of the control center. Thus, except the control center, no one can decrypt to obtain the amount. On the other hand, the homomorphic encryption feature in our scheme allows a substation to aggregate request messages sent by smart appliances within its region but the substation does not need to know about those individual amount values.

4) Traceability: As shown in Section V-E, the control center has the ability to reveal the real identity of any smart appliance based on their pseudo identities.

VII. Simulation Results

We evaluate our PASS scheme by simulation. To the best of our knowledge, our scheme is the first to address end-to-end security issues in a smart grid network, so we compare the performance with and without our PASS scheme. The results show that when under attack, the PASS scheme can allow much more normal request messages to arrive successfully at the control center due to the effective filtering done by the substation of the region where the attack is launched. The delay induced by the PASS system is marginal.

A. Simulation models

Our simulation is based on NS-2 [14]. We consider a smart grid network covering a small city. The smart grid network has a hierarchical structure (see Figure 2 for a simplified topology). At the highest level, there is a control center maintained by the power operator (Node 12 in Figure 2). At the middle level, there are substations with each of them being responsible for one region (Nodes 9, 10 and 11 in Figure 2). At the lowest level, there are smart appliances (Nodes 0 to 8 in Figure 2). Note that we ignore smart meters here since the communication between smart appliances and smart meters is not a focus of this paper. To simulate the nature of single incoming interface for all substations and control center, we connect a router node to each substation and control center for accepting traffic from lower levels (Nodes 13 to 16 in Figure 2).

For all of our experiments, we assume that the city consists of 10 regions (i.e. 10 substations) and the number of smart appliances is evenly distributed into the 10 regions where the number of smart appliances is a variable. Note that there may be far more smart appliances in a region but we only consider those which have power requests during the simulation period.

Each smart appliance is connected to the router node of the substation in its region via a wired link with bandwidth

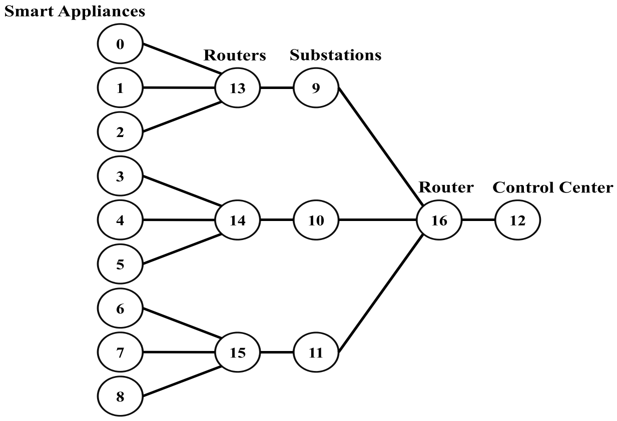

Fig. 2. A Simplified Topology

10 Mb/s. For the smart appliances that issue attack packets (attacking smart appliances), to ensure that all attacking traffic can reach the substation, the bandwidth of the wired links concerned is set to 10 Mb/s. Each substation is in turn connected to the router node of the control center via a wired link with bandwidth 10 Mb/s. The buffer size of each link is set to 10 packets and Drop Tail mechanism is applied whenever the buffer is full. For all power request messages, following the DNP3 frame structure in SCADA [15], we assume that the packet size is 250 bytes and with our PASS scheme, a 20-byte HMAC signature is added to each packet. All request messages are transmitted at a rate of 1 Mb/s. Since power request messages are assumed to be critical, UDP protocol is used for the transmission layer. Also for our PASS scheme, all HMAC signature verification is done at substations. From our experiment on a conventional Pentium Dual Core desktop, the time required for computing an HMAC signature is 368 msec.

We use the following three measures to evaluate the system.

1) Normal traffic success rate: which is defined as the proportion of normal power request messages sent by non-attacking smart appliances that can reach the control center within the simulation period.

2) Average delay: which is defined as the average duration from when a normal (non-attacking) smart appliance sends out its power request message to when the control center receives the message. Only requests that can reach the control center successfully are considered.

3) Total amount of data: which is defined as the total number of bytes of data being injected into the smart grid network for all power requests (including those being dropped) to reflect the amount of bandwidth wasted due to the attack. Attacking traffic sent by attackers is not included.

We consider a number of scenarios and each scenario lasts for 60 seconds (i.e. 1 minute) of NS time. We perform two sets of experiments. In the first set of experiments, we assume that there is no attacking traffic (i.e. no attacker) in the smart grid network. Within the 60 seconds of simulation time, there are random number of power request messages sent from smart appliances. The exact time of power request message generation is randomly chosen. This simulates different levels of traffic loading of the smart grid network. We then investigate the delay induced by the system. Since there is no attack packet, the total amount of data injected into the sytem is the total amount of data for all the request messages. With the PASS scheme, the overhead is only 20 bytes (for the HMAC signature) which is only 8% more compared to the case without the PASS scheme.

In the second set of experiments, we fix the number of smart appliances to 1000 (i.e. keep an identical traffic loading) and vary the number of attackers and the volume of attacking traffic to investigate their impact on normal power request messages sent by non-attacking smart appliances.

B. Simulation results and discussion

In the first set of experiments, we assume that there is no attacker in the smart grid network. We vary the total number of smart appliances from 500 to 5000 in steps of 500 to simulate different levels of traffic loading of the network. We then study the average delay experienced by each request with and without PASS and the result is shown in Figure 3. From the figure, we can see that the average delay (which includes transmission delay, propagation delay and queuing delay) slightly increases as the traffic loading of the network increases. With the PASS scheme, an additional 0.05 msec is required for the transmission due to the inclusion of 20 bytes of HMAC signature for each power request message.

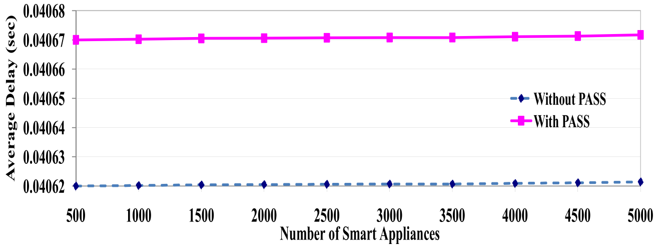

Fig. 3. Average Delay vs. Number of Smart Appliances

In the second set of experiments, we fix the number of smart appliances to 1,000. We then vary the number of attackers from 0 to 20 in steps of 1 and each attacker sends out attacking traffic at a transmission rate of 4 Mb/s (i.e. 4 times that of normal traffic) throughout the whole simulation period. Also we assume that all attackers concentrate in one region. For each number of attackers, we study the normal traffic success rate with and without PASS and the result is shown in Figure 4. From the figure, we can see that 3 attackers can already saturate the network in our case. Without PASS, the overall normal traffic success rate drops significantly from 100% to 15.3% as the number of attackers increases from 2 to 3. When the number of attackers increases from 3 to 4, the rate further drops slightly from 15.3% to 15.2%. However, with PASS, the overall normal traffic success rate only drops a little bit from 100% to 98.5% as the number of attackers increases from

0 to 4. That is, our PASS scheme yields more than 6 times improvement. The reason is that all attacking traffic are filtered at the substation level and so they will not be forwarded to the control center and affect other normal users.

On the other hand, for the attacking region (i.e., the region with attackers) and the non-attacking regions (i.e., the regions without attackers) separately, we find that without PASS, the proportion of normal traffic from the attacking region that can reach the control center is larger than that from the non-attacking regions. This is because by default, the control center router will schedule to transmit more packets from the attacking region due to the long queue on the corresponding incoming interface. With PASS, the normal traffic success rate in the attacking region increases a bit from around 78% to around 84% since attacking traffic will not compete for the outgoing link towards the control center anymore. The normal traffic success rate in the non-attacking region increases from 8.6% to 100% due to the attacking traffic filtering mechanism at substations in our scheme.

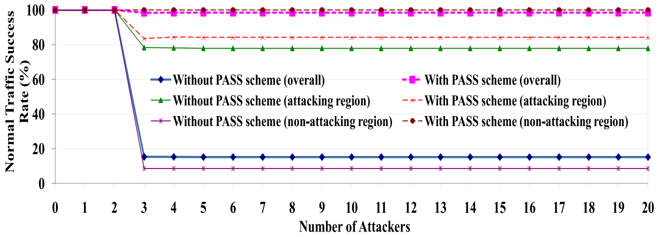

Fig. 4. Normal Traffic Success Rate vs. Number of Attackers

Regarding the delay performance under attack, with or without PASS, the overall average delay, the delay experienced by requests from attacking and non-attacking regions are quite close to each other. With PASS, each request experiences an average delay of 409 msec. Without PASS, each request experiences an average delay of 41 msec. That is, our PASS scheme only requires an additional 368 msec for HMAC signature verification at a substation.

From the above results, we can see that PASS yields significant gain in overall normal traffic success rate when under attack. The gain can be up to 6 times that without PASS. Though our scheme induces a small additional transmission delay (0.05 msec on average) and an HMAC signature verification delay (368 msec), this additional delay should be acceptable.

VIII. Conclusions

In this paper, we propose a privacy-preserving authentication scheme for the smart grid network. By observing that substations are usually physically harder to be compromised, they are utilized to help authenticate messages sent by smart appliances before these messages actually reach the control center. We suggest to connect smart appliances to tamper-resistant devices which are assumed to be secure from data cracking or operation disturbance, which makes it feasible for the substation to distinguish attack packets from normal requests. A major feature of our scheme is that the privacy of any customer including their daily electricity usage can be preserved while at the same time the control center can generate a proper amount of electricity.

Through our simulation study, we showed that with our PASS scheme, the additional transmission delay induced is 0.05 msec on the average while the HMAC signature verification delay induced is 368 msec only. On the other hand, the message overhead is only 20 bytes per request message. When under attack, our scheme yields a significant gain in normal traffic success rate especially in non-attacking regions and the gain can be up to more than 6 times. This shows the effectiveness of our filtering mechanism at substations. In the future, we will implement our scheme in a testbed. If we can collect statistics on real power usage, we could perform a more realistic simulation. There is one limitation in our scheme, the success rate in the attacking region drops due to the time used for the authentication of the attack packets. To tackle this issue, one possible direction is to re-route some of the packets to the nearby substations whenever the volume of requests exceeds a certain threshold so that the workload can be shared by other substations. Besides, we are considering other secure applications in smart grid networks.

References

[1] J. Northcote-Green and R. Wilson, "Control and Automation of Electrical Power Distribution Systems," 2006.

[2] ARC Advisory Group, "SCADA Systems for Smart Grid," http://www.arcweb.com/Research/Studies/Pages/SCADA-Power.aspx.

[3] H. Khurana, M. Hadley, N. Lu, and D.A. Frincke, "Smart-Grid Security Issues," *IEEE Security and Privacy magazine*, pp. 81 – 85, Feb. 2010.

[4] The Smart Grid Interoperability Panel Cyber Security Working Group, "Second Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements," Feb. 2010.

[5] Office of the National Coordinator for Smart Grid Interoperability, "NIST Special Publication 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0," Jan. 2010.

[6] SmartGrids, "European SmartGrids Technology Platform: Vision and Strategy for Europe's Electricity Networks of the Future," *European Commission, Directorate-General for Research, Sustainable Energy Systems, EUR 22040*, 2006.

[7] Electric Power Research Institute, "Intelligrid," http://intelligrid.epri.com/.

[8] US Department of Energy, "Grid 2030: A National Vision for Electricity's Second 100 Years," 2003.

[9] V.O.K. Li, F.F. Wu, and J. Zhong, "Communication requirements for Risk-Limiting Dispatch in Smart Grid," in *Proceedings of the IEEE Workshop on Smart Grid Communications*, May 2010.

[10] Juniper Networks Inc., "Architecture for Secure SCADA and Distributed Control System Networks," 2009.

[11] B. Kaliski and J. Staddon, "RSA Cryptography Specifications Version 2.0," *IETF RFC2437*, 1998.

[12] D. Eastlake and P. Jones, "US Secure Hash Algorithm 1 (SHA1)," *IETF RFC3174*, 2001.

[13] R. Rivest, "The MD5 Message-Digest Algorithm," *IETF RFC1321*, 1992.

[14] Information Sciences Institute, "Network Simulator (NS) 2," http://www.isi.edu/nsnam/ns/.

[15] e nor.net, "IEC 60870 and DNP3 - the middle layers," http://my-web-base.com/e-nor/scada-2.htm.

Acknowledgement

This research is supported in part by the Collaborative Research Fund of the Research Grants Council of Hong Kong under Grant No. HKU10/CRF/10.