2011

A Secure and Reliable In-network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid

Yun Ye
University of Nebraska-Lincoln, yye@huskers.unl.edu

Yi Qian
University of Nebraska-Lincoln, yqian2@unl.edu

Hamid Sharif
University of Nebraska-Lincoln, hsharif@unlnotes.unl.edu

IEEE WCNC 2011 - Network
2011 IEEE Wireless Communications and Networking Conference (WCNC)
doi: 10.1109/WCNC.2011.5779257

A Secure and Reliable In-network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid

Ye Yan, Yi Qian and Hamid Sharif
Department of Computer and Electronics Engineering
University of Nebraska-Lincoln
Emails: yy2318@ieee.org, {yqian2, hshari}@unl.edu

***Abstract*—We consider various security vulnerabilities of deploying Advanced Metering Infrastructure (AMI) in smart grid, and explore the issues related to confidentiality for customer privacy and customer behavior as well as message authentication for meter reading and control messages. There are only a very few research work on AMI authentications, and no work exists on confidentiality for user privacy and user behavior, from the best of our knowledge. In this paper, we propose an in-network collaborative scheme to provide secure and reliable AMI communications in smart grid, with smart meters interconnected through a multihop wireless network. In this approach, an AMI system can provide trust services, data privacy and integrity by mutual authentications whenever a new smart meter initiates and joins the smart grid AMI network. Data integrity and confidentiality are fulfilled through message authentication and encryption services respectively using the corresponding keys established in the mutual authentications. A transmission scheme is proposed to facilitate the data collection and management message delivery between smart meters and a local collector for AMI communications. Simulation results show that the proposed method has a better end-to-end delay and packet losses comparing with a basic security method, and the proposed method can provide secure and reliable communications for AMI in smart grid systems.**

***Index Terms*—Advanced metering infrastructure (AMI), multihop wireless network, security, smart grid**

I. Introduction

Smart grid delivers electricity between suppliers and consumers using two-way digital technology to control intelligent appliances at consumers' home or building to save energy, reduce cost and increase reliability, efficiency and transparency [1] [2]. Smart grid is characterized by a two-way flow of electricity and information to create an automated, widely distributed delivery network. It incorporates into the electricity grid the benefits of communications to deliver real-time information and enable the near-instantaneous balance of supply and demand [3] [4]. According to the Electric Power Research Institute (EPRI), one of the emergent requirements facing the smart grid development is related to cyber security of the system. As indicated in the EPRI report [5], cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways.

Advanced Metering Infrastructure (AMI) refers to systems that collect, measure and analyze energy usage, from networks that connected to next-generation electricity meters, or, smart meters. An AMI includes software, hardware, communication networks, customer-associated systems and meter data management (MDM) software. As the smart grid becomes reality, security threats grow exponentially, from inside and outside of the system. Utilities will almost certainly face substantial liability claims and regulatory fines if inadequate security technologies enable eavesdroppers, adversaries or hackers to acquire and use AMI data to a customer's detriment, or worse, interrupt service or hold utility customers "hostage". Furthermore, if customers believe a utility is abusing personally identifiable data, or is generally collecting information beyond what they deem acceptable (whether or not legal), then they are likely to resist the implementation of AMI. Consumers may refuse to consent (where required), hide their data or pursue political opposition. Therefore, confidentiality for user privacy and user behavior and authentication for meter reading and control messages, are two of the major security services need to be provided before an AMI can be deployed in smart grid systems. From our recent survey on smart grid communication infrastructures and on cyber security for smart grid communications [6] [7], there are only a very few research work on AMI authentications, e.g., [8]–[13], and no work exists on confidentiality for user privacy and user behavior, from the best of our knowledge.

In this paper, we develop an integrated confidentiality and authentication scheme for secure and reliable AMI communications for smart grid systems. First, we develop a mutual device authentication procedure for the proposed in-network collaborative scheme which establishes the security key pairs for AMI communications. Then we provide an in-network collaborative scheme between smart meters and a local data collector/dispersion point to fulfill the secure and reliable communications for meter-reading collections and manage-

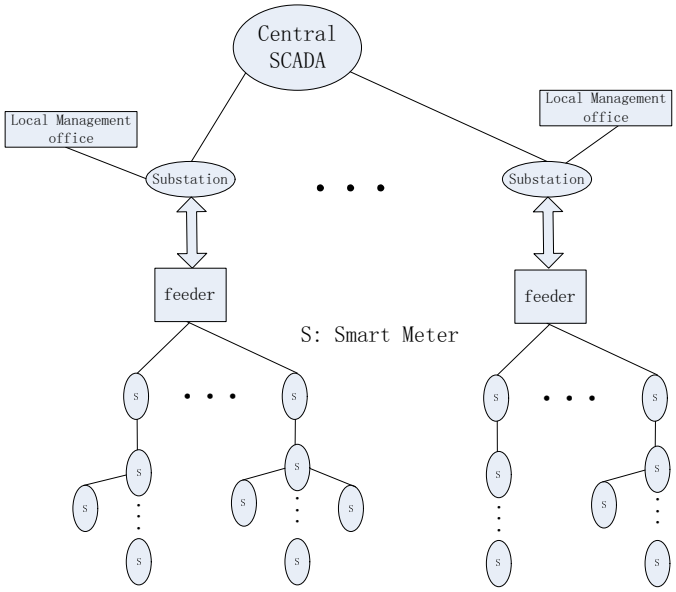

Fig. 1. A Smart Grid AMI Communication System Architecture

ment messages. We evaluate the performance of the proposed secure and reliable in-network communication scheme through simulations.

The rest of this paper is organized as follows. Section II provides a brief description of the smart grid AMI communication system model. Section III discusses briefly cyber security requirements for AMI in smart grid. Section IV gives the details of the proposed in-network collaborative communication scheme for AMI in smart grid. Section V presents simulation results for the proposed in-network collaborative communication scheme. Section VI draws the conclusion.

II. Smart Grid AMI Communication System Architecture

Fig.1 shows a commonly used communication architecture for smart grid AMI, which is generalized from the literature [6] [7] [9] [11] [14].

The Supervisory Control and Data Acquisition (SCADA) systems have been implemented to monitor and control electrical power grids for decades [15]. The central SCADA manages the electricity supply to substations on high voltage ($>$ 230 KV) transmission lines. Usually, the handoff from high voltage electricity transmission to middle voltage (11 KV) electricity distribution for feeder lines takes place in substations. After the voltage transformation at the end of the feeder line, a consumer terminal can get the properly low voltage (110 V/220 V) electricity at home. At each home, the smart meter collecting the electricity power consumption data from all intelligent appliances at home online and send them back to local management office of the utility company. Those data are processed as billing information and aggregated, and then forwarded to SCADA for the utility operator. With this real-time power consumption information from terminal consumers, the utility operator can monitor and diagnose the on-line statues of the whole smart grid system, then optimally adjust the power generation, transmission and distribution according to the power quality, and to smooth the peak demand and further avoid the potential blackout at the utility side. The real-time management messages will be distributed to corresponding costumers backward to smart meters through the AMI system. Therefore, the intelligent appliances re-schedule their tasks and working periods accordingly to avoid the rush hours in power demand and further to reduce the blackout chances at the consumer side.

In the architecture shown in Fig.1, the communication infrastructure for the low voltage electricity distribution network is usually implemented by wireless technologies such as IEEE 802.11 Wi-Fi, for a group of terminal consumers. For simplicity, each terminal consumer is considered to be represented as a smart meter, and all the intelligent appliances of a home is covered by a smart meter, i.e, a smart meter is a home portal for AMI communications in smart grid. These smart meters are connected to a feeder line which acts as a gateway and leads the collected meter-reading to the local management office at the back side of substation using IEEE 802.16 WiMax technology. At the local management office, the smart meter-reading is recorded for individual customer and aggregated to further forward to central SCADA for system monitoring, demand managing, operation optimizing, using dedicated fibre optical connections.

In Fig.1, the communication technology to be deployed between smart meters and the feeder can be a multi-hop wireless network, because wireless networking is the most economical way to connect a group of distributed smart meters in a community [16]. For a multi-hop wireless network, a wireless backbone routing scheme can be formed to connect the smart meters efficiently [17].

III. Cyber Security For AMI in Smart Grid

Currently for AMI in smart grid communications, it lacks sufficient work for security schemes including adequate authentication mechanisms. To the best of our knowledge, there is no practical mechanism to meet the scalability problem of the smart meter authentications. For example, to authenticate a smart meter as a Home Area Network gateway (HAN GW), another smart meter, a Building Area Network gateway (BAN GW) should communicate with the HAN GW securely. This communication needs to be encrypted with secret keys of BAN and HAN GWs. Meanwhile, the BAN GW should be authenticated with the Neighboring Area Network gateway (NAN GW) and the data flows among them should be encrypted as well.

The cryptographic overheads such as the digital certificate and signature take up a significant portion comparing to the process of the data packet itself. In addition, cryptographic operations also contribute to significant computational cost, especially in recipient end, which verifies the message. In smart grid, a smart meter typically send each meter-reading message within an interval of 500 ms. Generating a digital signature every 500 ms is not a serious problem for Public

Key Infrastructure (PKI) based digital signature schemes using a regular personal computer nowadays. However, for a legacy power grid system that connects hundreds of buildings, each of which may have a large number of apartments, the number of meter-reading messages that require to be verified by the NAN GW might be significantly huger than its capacity.

In addition, the smart meters are vulnerable to various cyber attacks found in the literature. The use of wireless and IP technologies enable the online management facility meanwhile make smart grid AMI communications more vulnerable to cyber attackers.

Digital signing and verifying each message can certainly achieve secure communications indeed. However, we find the conventional cryptographic operations make such security schemes neither scalable nor affordable to the traffic density and system resource constraints in smart grid. Since most conventional security schemes such as PKI are not adequate for the stringent requirement of smart grid AMI communications. Consequently, we need to come up with some light-weight but still secure enough verification schemes tailored for the specific smart grid AMI communications so the meter-reading collections and management messages can be processed securely and fasterly.

IV. An In-network Collaborative Communication Scheme

In order to address the afore mentioned cyber security threats, we have developed an in-network collaborative scheme for AMI which can provide secure and reliable communications. The design objectives of the proposed in-network collaborative communication scheme is discussed in the following.

1) Device authentication: The identity and legality of the smart meters and the associated consumers should be verified before joining the interconnected smart meter network and receiving the proper utility service.
2) Data confidentiality: The smart meter readings and management control messages should be kept in confidential to conceal consumers' privacy and utilities' business information from unauthorized entities.
3) Message integrity: The smart grid should be able to verify that any meter-reading/management messages to be delivered unaltered in AMI.
4) Maintaining secrecy: It should be ensured that some secrecy of a smart meter will always keep in privacy while some secrecy should be shared with particular partners to build secure communications.
5) Prevent potential cyber attacks: A smart meter, by holding its own digital credential and following certain processes in the proposed in-network collaborative scheme, should be guaranteed to obtain secure communication connections with the smart meter network. Even if an individual smart meter is compromised, the adversary cannot use the compromised smart meter to further access other smart meters' information or take the advantage to penetrate the AMI in smart grid.

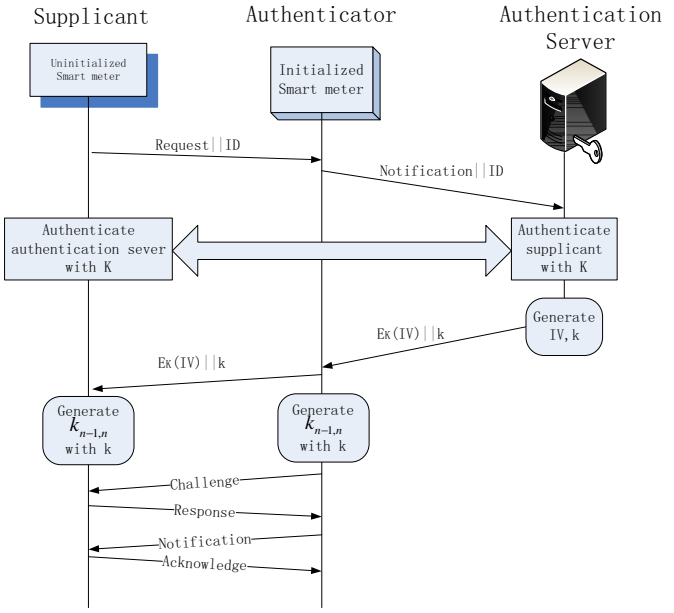

Fig. 2. Initialization Process for A Newly Boot-up Smart Meter

6) Facilitating communication overhead: Any security scheme will bring additional system overhead especially in communications. The proposed in-network collaborative communication scheme should be efficient in terms of communication overhead and processing latency.

A. Initialization Process

Fig.2 illustrates the initialization process for each newly boot-up smart meter as a supplicant in the mutual authentication. Before joining the authenticated smart meter network, it must be authenticated by the remote authentication server located at the local management office as a legal device and terminal customer. The neighboring authenticated smart meter plays as a authenticator in the initialization process to convey the authentication process message between the supplicant and the authentication server. Both the supplicant and the authentication server have an identical key K, which is never concealed to anyone else including the authenticator. Because both the mutual authentication identities and the consequent data encrption/decrption between supplicant and authentication server are based on this K. If the supplicant's identity is authenticated as a valid device, the corresponding credential of the supplicant is established between the authentication server and the supplicant. Then, authentication server will generate an initiate vector (IV) and a key k. The IV and k will be encrypted by K, so the supplicant can decrypt and get its IV and k. Meanwhile, the authentication server sends the k to the authenticator encrypted with their own K' since authenticator was authenticated already with K'. So the authenticator know the k. With its k, the supplicant and authenticator can generate the $k_{n-1,n}$ individually then conduct a four-way handshake procedure to fulfill another mutual authentication between supplicant and authenticator.

After the successful mutual authentication, $k_{n-1,n}$ at both supplicant and authenticator sides are validated and ready for the consequent message authentication code generation and validation purpose.

Since every smart meter must fulfil the initialization process, the back-end authentication server can collect all the necessary topology information of the multihop wireless smart meter network. The back-end server can generate the optimal routing backbone as discussed in [17] and notify the correspond smart meters on the existing backbone as well as the newly initiated smart meter dynamically. In the rest of this paper, we examine secure and reliable communications under the assumption that a group of smart meters forms a route chain topology with the orders node 1, node 2, ..., node n, and the collecting node, which is a logic assumption from the studies in [17].

B. In-network Meter-reading Collection Process

Fig.3 illustrates the encryption/decryption and message authentication process for meter reading collection in AMI environment. The smart meter node 1, which is at the beginning of a route chain, conducts an XOR operation using its meter-reading message in plain text with its own IV. Then, it uses the result as the input of the encryption associated with its K_1 to generate the encrypted message M_1. The message authentication operation uses M_1 and $k_{1,2}$ to generate the corresponding message authentication code which will be appended to M_1. Then, both M_1 and the corresponding message authentication code will send to its neighboring smart meter node 2, the next hop along the route to the collecting node.

The smart meter node 2 generates its own message authentication code with $k_{1,2}$ and the received M_1. If the generated message authentication code matches the received one, the integrity of the received M_1 is verified. Then, M_1 is integrated and run as the input of XOR operation with the meter reading of smart meter node 2. The similar process takes place in all the intermediate nodes in the route chain until it reach the collecting node, which have all the K_n in the route. After the message authentication validated with the smart meter node n, the collecting node can decrypt all the meter readings from smart meter node 1 to smart meter node n on the route chain at once.

The collecting node will aggregate the received meter-readings and forward these processed data through dedicated lines or an overlay network to uplinks. All the meter-readings on feeder lines are collected in local management office where the real-time meter-readings are reordered for billing purpose. Besides that, the information extracted from the real-time meter-readings will be utilized not only by both local management office and/or substation, but also by central SCADA system operation.

C. In-network Management Message Distribution Process

Since the remote central SCADA and local management office/substation will adjust the power generation, transmission and distribution in smart grid according to the collected meter-readings. The management and control messages will be distributed to specific smart meters to schedule the intelligent home appliance operations correspondingly.

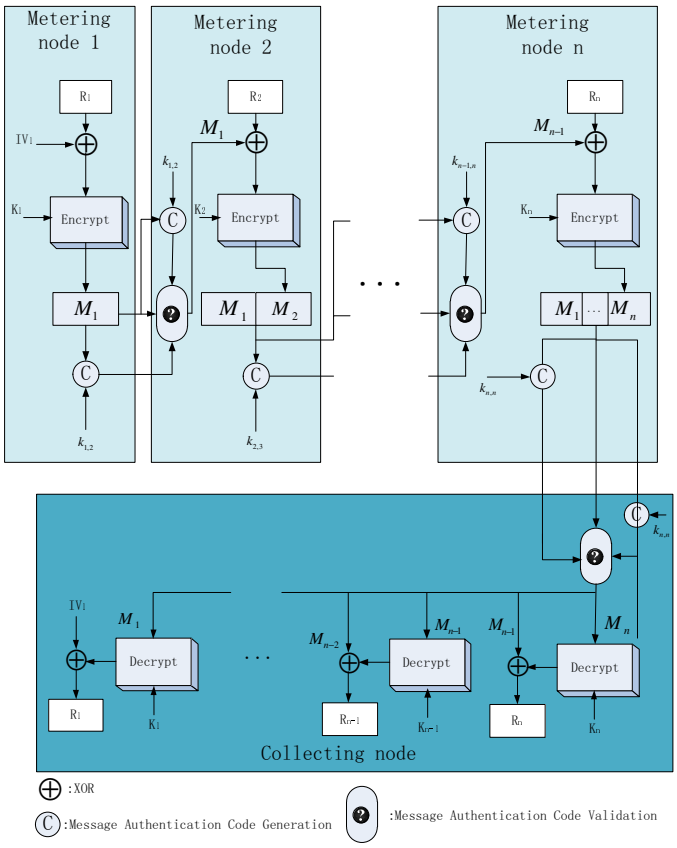

Fig. 3. In-network Meter-reading Collection Process

Fig.4 shows the reverse process flow comparing with Fig.3, which can be used to cast the specific management messages from collection node to particular smart meter nodes on the chain topology route. We call our proposed AMI security scheme the "in-network" security scheme since both the authentication and the encryption processes are performed hop-by-hop in the communication route.

V. Performance Evaluations

We evaluate the performance of our proposed in-network collaborative communication scheme in AMI by simulations using ns-2. In the simulation results shown here, we test two scenarios, with 5-node and 10-node smart meters in the route chain to the collecting node, and the collecting node is equipped with a PC processor while each of the smart meter nodes is associated with an ARM processor. The wireless channel between any two neighboring nodes are under the effect of shadow fading. The transmit power of nodes is set to the minimum value that ensures successful transmissions between only two immediate nodes so there is no interference to other nodes. The uplink traffic due to meter-reading is simulated by letting each meter node generating a constant-bit-rate (CBR) session with destination to the collecting node using UDP at the rate 1 packet/second with the packet size

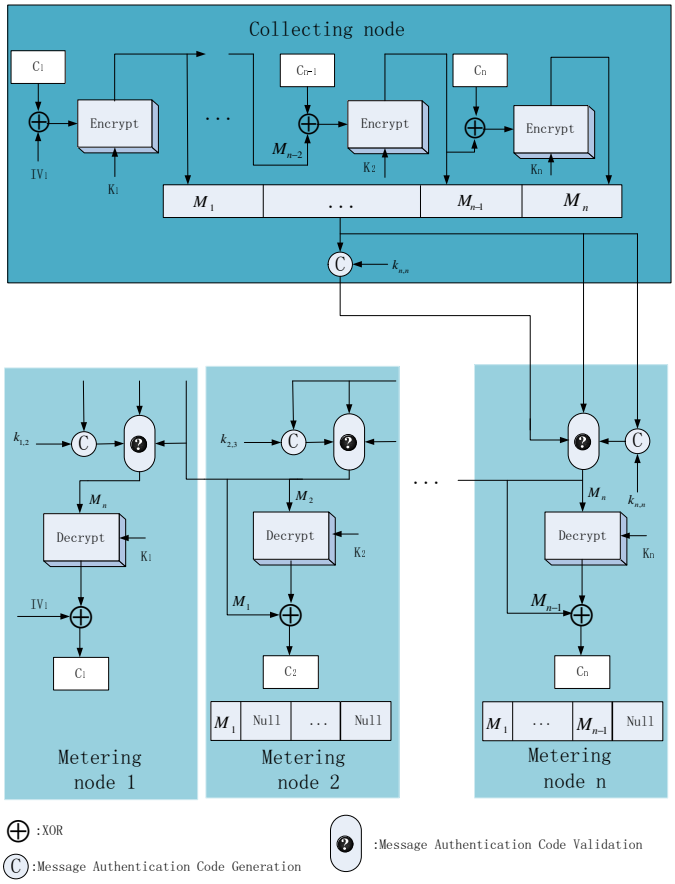

Fig. 4. In-network Control Message Distribution Process

50 bytes. The encryption/decryption (SEED) and message authentication code generation (HMAC) time consumption listed in Table I is added to each smart meter node and the back-end collecting node accordingly [18]. The simulation

TABLE I
MESSAGE PROCESSING TIME FOR ARM AND PC [18]

Process	Processing time on ARM	Processing time on PC
SEED	19.23 μs	3.4 μs
HMAC	23.63 μs	3.68 μs

results from Fig.5 to Fig.8 illustrate the performance of the proposed AMI "in-network" security scheme. On each of the figures it also compares with the results of a basic security approach that each of the smart meters will communicate to the collecting node through a private key and an independent end-to-end encryption (in which we call it "basic security scheme", or simply "basic scheme"). End-to-end delay is a crucial performance parameter for real time applications such as on-line reading collection for electricity voltage, current, phase and reactive power status in smart grid. If the data cannot meet its end-to-end deadline, it will be useless for on-line meter readings. Consequently it might cause serious system fault especially in monitoring/protecting system for missing the fault detection. While packet drop rate is another important

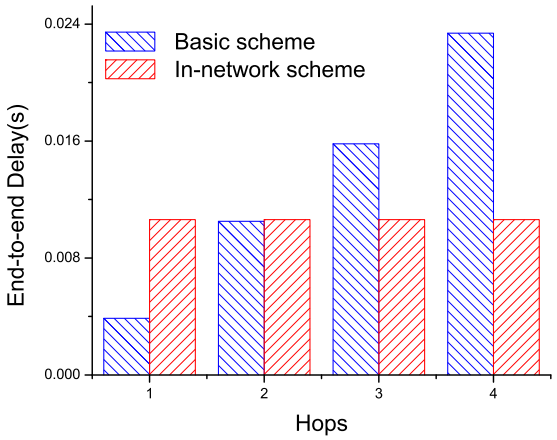

Fig. 5. End-to-end Delay (Second) vs. Hops Counts in 4 hops

performance parameter for the system to make prompt and proper decision based on the on-line real-time meter readings and data collections.

Fig.5 and Fig.6 show that the proposed in-network security scheme is superior to the basic security scheme as the hop count increasing. The wireless interference is getting worse as more and more wireless devices involved simultaneously, our proposed approach can be arranged in a transmission schedule for each participated smart meter at its initialization process. Therefore, all the participated smart meters will transmit in a pre-define order to avoid the interference in both transmitting and receiving. So after all the participated smart meters finish their own receiving and transmitting schemes without any interference, the whole process is accomplished. That is why our proposed approach can achieve identical low end-to-end delay while the basic security scheme getting worse and worse as the hop count increasing.

Fig.7 and Fig.8 shows the significant differences on packet drop performance. The proposed in-network scheme can keep in very low (almost 0%) packet drop rate while the basic security scheme performance degrades dramatically as the hop count increasing. It is beyond 20% as the hop count reaches 9 which is obviously impairing its operation of applications such as on-line meter reading, monitoring and/or protecting.

VI. CONCLUSION

As a critical part of the smart grid communication infrastructure, AMI is expected to face a variety of security threats which not only targeting the smart meters in AMI, but also impairing the reliability of smart grid operations. In this paper, we investigate cyber security problems of deploying AMI in smart grid. In particular, we propose a secure and reliable in-network collaborative communication scheme for AMI in smart grid. Our proposed in-network approach employs mutual authentications with a remote authentication server located in local management and a neighboring smart

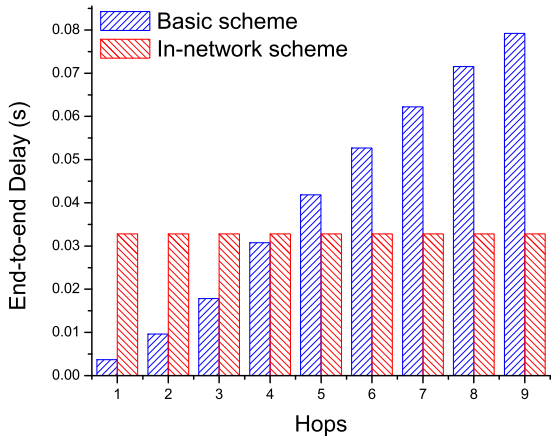

Fig. 6. End-to-end Delay (Second) vs. Hops Counts in 9 Hops

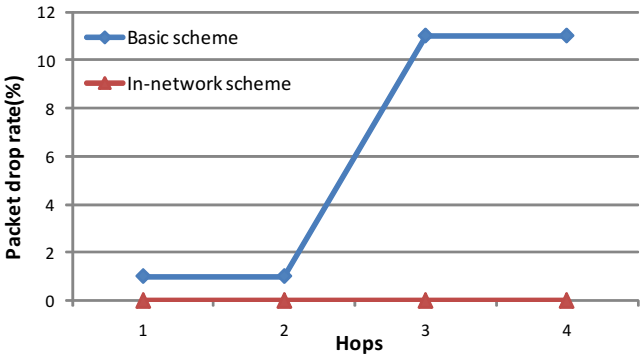

Fig. 7. Packet Drop Rate (%) vs. Hop Counts in 4 Hops

meter as the authenticator to get the proper cryptography keys for consequent secure data communications. Therefore, the meter readings from smart meters and management messages from central SCADA and/or local management office employ encryption and message authentication mechanisms tailored for both the security requirements and system constraints. The performance of the proposed security scheme is verified through simulations. We show that the proposed method has a better end-to-end delay and packet losses comparing with a basic security method, and the proposed method can provide secure and reliable communications for AMI in smart grid systems.

REFERENCES

[1] U. S. Department of Energy, [online] Available: www.oe.energy.gov.

[2] "Smart grid," [online] Available: http://en.wikipedia.org/wiki/Smart grid.

[3] F. Rahimi and A. Ipakchi, "Demand response as a market resource under the smart grid paradigm," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 82–88, 2010.

[4] L. Fangxing, Q. Wei, S. Hongbin, W. Hui, W. Jianhui, X. Yan, X. Zhao, and Z. Pei, "Smart transmission grid: Vision and framework," *IEEE Transactions on Smart Grid* , vol. 1, no. 2, pp. 168–177, 2010.

[5] Electric Power Research Institute, "Report to nist on smart grid interoperability standards roadmap," 2009.

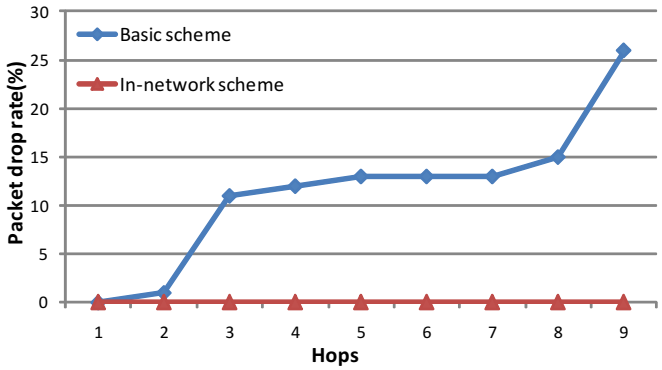

Fig. 8. Packet Drop Rate (%) vs. Hop Counts in 9 Hops

[6] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," submitted to publications.

[7] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," submitted to publications.

[8] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century,* pp. 1–5, 2008.

[9] H. Cheung, A. Hamlyn, and Y. Cungang, "Network security authentication of power system operations," in *Canadian Conference on Electrical and Computer Engineering (CCECE 2008)*, pp. 687–692, 2008.

[10] S. Fries, H. J. Hof, and M. Seewald, "Enhancing iec 62351 to improve security for energy automation in smart grid environments," in *Fifth International Conference on Internet and Web Applications and Services (ICIW 2010),* pp. 135–142, 2010.

[11] T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, and K. Sekiguchi, "Information-theoretic approach to authentication codes for power system communications," in *IEEE Transmission and Distribution Conference and Exposition,* pp. 1–7, 2010.

[12] Z. Sun, S. Huo, Y. Ma, and F. Sun, "Security mechanism for smart distribution grid using ethernet passive optical network," in *2nd International Conference on Advanced Computer Control (ICACC 2010)*, vol. 3, pp. 246–250, 2010.

[13] A. Hamlyn, H. Cheung, T. Mander, W. Lin, Y. Cungang, and R. Cheung, "Computer network security management and authentication of smart grids operations," in *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century,* pp. 1–7, 2008.

[14] A. Aggarwal, S. Kunta, and P. K. Verma, "A proposed communications infrastructure for the smart grid," in *Innovative Smart Grid Technologies (ISGT 2010),* pp. 1–5, 2010.

[15] G. A. Taylor, M. R. Irving, P. R. Hobson, C. Huang, P. Kyberd, and R. J. Taylor, "Distributed monitoring and control of future power systems via grid computing," in *IEEE Power Engineering Society General Meeting*, 2006.

[16] Wireless Design and Development, "Front end module for advanced metering infrastructure and other 900 mhz ism band applications." [online] Available: http://www.wirelessdesignmag.com.

[17] H. Guo, Y. Qian, K. Lu and N. Moayeri, "Backbone Construction for Heterogeneous Wireless Ad Hoc Networks," IEEE International Conference on Communications, 2009 (ICC'09), pp.1-5, June 14-18, 2009

[18] S. Hong, M. Lee, D. Shin, "Experiments for Embedded Protection Device for Secure SCADA Communication," Asia-Pacific Power and Energy Engineering Conference (APPEEC 2010), pp.1-4, March 28-31, 2010