Secure and energy-efficient multicast routing in smart grids

Secure and Energy-Efficient Multicast Routing in Smart Grids

Bashar Ahmed Alohali*, Vassilios G. Vassialkis†
* School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, U.K.
† Dept. of Electronic Engineering, University of Surrey, Guildford, U.K.

***Abstract*—A smart grid is a power system that uses information and communication technology to operate, monitor, and control data flows between the power generating source and the end user. It aims at high efficiency, reliability, and sustainability of the electricity supply process that is provided by the utility centre and is distributed from generation stations to clients. To this end, energy-efficient multicast communication is an important requirement to serve a group of residents in a neighbourhood. However, the multicast routing introduces new challenges in terms of secure operation of the smart grid and user privacy. In this paper, after having analysed the security threats for multicast-enabled smart grids, we propose a novel multicast routing protocol that is both sufficiently secure and energy efficient. We also evaluate the performance of the proposed protocol by means of computer simulations, in terms of its energy-efficient operation.**

***Keywords*—Smart Grid; Secure Routing; Multicast.**

I. Introduction

Smart grid (SG) is a modernized electrical grid that operates with sensors and *smart devices* (SDs). It uses advanced communication and control technologies for monitoring and automation to enable flexible, efficient, and reliable power delivery and distribution [1], [2]. Due to significant heterogeneity of devices and communication technologies used in SGs, they are more vulnerable to security threats and attacks compared with traditional communication networks [3]. The proposed methods for securing SG devices and infrastructure against security attacks include access control, host intrusion detection, and system hardening. However, the integration of cyber technology with the SGs and industrial control systems reveals new security vulnerabilities and attack threats [4], [5].

Furthermore, multicast routing has been recognized as an important requirement for SGs to enable efficient data exchange between utility management software and groups of *smart meters* (SMs) [6], [7]. Some examples of multicast routing applications in SGs include monitoring and protection, requests for periodic meter readings, and demand-response programs [9], [8]. However, the multicast routing introduces new challenges in terms of secure operation of the smart grid and user privacy. Although some works that study these problems have recently appeared in the literature, there are still some remaining issues to be addressed [10].

In this paper, we introduce a novel multicast routing protocol that is both sufficiently secure and energy efficient. We describe both, the authentication phase and the communication phase. The authentication phase, registers a group of SMs with a network entity called *group controller* (GC) that acts as certificate authority. After that, during the communication phase, SMs periodically collect energy consumption information for SDs and send the aggregated consumption information to the *network operations centre* (NOC). The latter is located at the utility network side and is responsible for the control and operation of SG. Also, from time to time, NOC sends control messages to SMs, e.g. instructing them to reduce the home energy consumption during the peak hours. Finally, we evaluate the proposed protocol in terms of its energy-efficient operation.

This paper is structured as follows. In Section II, we review the relevant works on secure communications for SGs. In Section III, we describe the considered network model for SG. In Section IV, we describe our proposed secure multicast protocol. In Section V, we evaluate the performance of the proposed protocol by means of computer simulations. Finally, we conclude in Section VI.

II. Related Work

In this section, we review current research works related to SG security, authentication, and key management.

A number of works propose secure communication protocols for SGs. Khurana *et al.* [11] describe the design principles for SG cyber-infrastructure authentication protocols. They point out that the design of an authentication mechanism for SG is a challenging task and is prone to significant errors if not done carefully. Kim *et al.* [12] propose a protocol for secure unicast, multicast, and broadcast communications in SG. This protocol applies a binary tree approach and aims at reducing the computational overhead. However, the proposed approach does not provide sufficient security when one or more nodes join or leave the session, as may happen, e.g., in case of node failures. Li *et al.* [13] propose a distributed data aggregation approach for SG. According to this approach, multiple smart meters are involved in aggregation and routing to the collector unit. To achieve secure routing and to protect user privacy, homomorphic encryption is used. However, this approach does not protect against replay attacks and against malicious manipulation of aggregated data.

Key management and authentication schemes for SGs have also attracted some research efforts. Wu *et al.* [14] propose a key management scheme for SG. The proposed scheme is based on public keys and secures against man-in-the-middle and replay attacks. However, both public-key infrastructure and third-party trusted anchors are required. This increases the complexity of the overall solution and also does not perform well in case of multicasting. Nicanfar *et al.* [15] proposed a key management protocol for data communication between the

TABLE I. ABBREVIATIONS

AMI	Advanced Metering Infrastructure
FAN	Field Area Network
GC	Group Controller
HAN	Home Area Network
NAN	Neighbourhood Area Network
NOC	Network Operations Centre
PKI	Public-Key Infrastructure
SD	Smart Device
SDD	Smart Device with Duplex communication
SDS	Smart Device with Simplex communication
SG	Smart Grid
SM	Smart Meter
SN	Serial Number
UKMF	Unified Key Management Framework
WAN	Wide Area Network

utility server and SMs. However, the authentication method between the SM and the home appliances has not been addressed. Das *et al.* [16] proposed a unified key management framework (UKMF) for cross-layer peer entity authentication. This mechanism has applicability in SGs, especially for smart metering, where SMs are assumed to be low-cost wireless devices for which repeated peer entity authentication attempts for each protocol can be contributed to increased system overhead. The proposed mechanism is flexible in that peer entity authentication can be treated as either network access authentication or application-level authentication. However, the bootstrap application ciphering is an important and as yet missing piece to realizing the unified key management framework vision. Yee *et al.* [17] proposed a key management scheme for a wide-area measurement system in SG. The scheme is targeting a concrete set of security objectives derived from NIST's security impact level ratings. The authors identify multicast authentication as the primary challenge. Li *et al.* [18] identify the requirements for multicast communication and multicast authentication in SG. They study the suitability of one-time signature for multicast authentication in SG and show that this solution results in short delays and low computational cost. However, the aforementioned gains are limited to the cases where receivers have limited storage or where the communication is frequent and short.

III. NETWORK MODEL

In this section, we describe our considered SG network architecture, comprising three tiers (Fig. 1). Next, we introduce some basic definitions and notations. Finally, we discuss three types of security attacks in SG and define the considered threat model.

All abbreviations used in the paper are listed in Table I.

A. Network Architecture

The considered SG architecture comprises three following tiers.

Tier 1: Home Area Network (HAN). A HAN connects the in-house SDs with a SM. A SM acts as a gateway between the in-house devices and the external parties. The electric utility manages the power distribution within the SG, collects sub-hourly power usage from SMs, and sends notifications to SMs when required. SM receives messages from devices within the HAN and sends them to the appropriate service provider

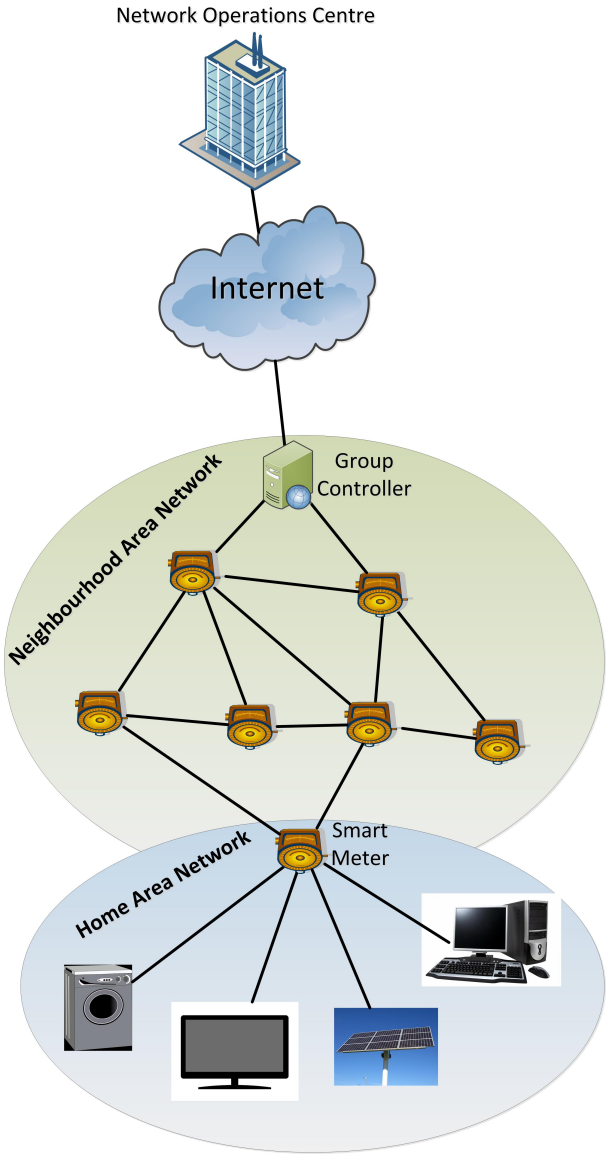

Fig. 1. Smart grid network model.

[24]. We assume a single SM per house and a star topology of multiple SDs with SM at the centre. The communication between SDs and SM is achieved via any appropriate and available technology, such as ZigBee [19], 6LoWPAN [20], wired or wireless Ethernet, Bluetooth [21], etc. We consider two types of home SDs:

- SDDs: devices that support *duplex* communication, i.e. that are able to both send and receive messages to and from SM.
- SDSs: devices that support *simplex* communication, i.e. that are able only to send messages to SM.

Tier 2: Neighbourhood Area Network (NAN). A NAN connects SMs to local access points (GCs) for Advanced Metering Infrastructure (AMI) applications [22]. This can be a network of SMs creating a mesh, as well as part of a mesh network, which consists of SMs and gateways that relay data. A version of the network, which is deployed to collect data

TABLE II. NOTATIONS

H_n	Number of houses in neighbourhood n
GC_n	Group controller of neighbourhood n
$SM_{h,n}$	Smart meter in house h and neighbourhood n
$I_{h,n}$	Number of duplex smart devices in house h and neighbourhood n
$J_{h,n}$	Number of simplex smart devices in house h and neighbourhood n
$SDD_{i,h,n}$	Duplex smart device i in house h and neighbourhood n
$SDS_{j,h,n}$	Simplex smart device j in house h and neighbourhood n
$E_{PubKeyGC}$	public key of group controller
ID_{SM}	Identity number of smart meter
$SymKey_{SM}$	Symmetric key shared between a smart meter and its group controller
ID_{GC}	Identity number of group controller
SN_{SM}	Serial number of smart meter
SN_{NSM}	Serial number of new smart meter
$E_{PubKeyPSM}$	Public key of proxy smart meter
$SymKey_{NSM}$	Symmetric key shared between a new smart meter and its group controller
$E_{SessKey}$	Session key shared between the group controller and all SMs of the group
$E_{PubKeyNOC}$	Public key of the network operations centre
TS	Timestamp

from power lines, mobile workforce, towers, etc., for power grid monitoring, is referred to as Field Area Network (FAN). In this paper, we will use NAN to refer to both types of networks. The coverage of a NAN is around $1-10$ square miles. The data rate would be higher than that of HANs, and in the order of $10-1000$ Kbps [6].

Tier 3: Wide Area Network (WAN). A WAN is a large network that connects GCs to the *network operations centre* (NOC) at the utility provider. The communication within a WAN can be performed using WiMax, GSM/WCDMA/LTE, or fibre optics [23].

B. Basic Definitions and Notations

The whole area of the SG is divided into N neighbourhoods. A neighbourhood $n(n = 1, ..., N)$ consists of H_n houses. Each house $h(h = 1, .., H_n)$ in a neighbourhood n has a smart meter, $SM_{h,n}$. Each neighbourhood n has an associated *group controller*, GC_n, that controls all SMs within this neighbourhood. SMs are connected to their GC_n either directly or indirectly (i.e., via other SMs). This effectively forms the NAN, as it was also described in previous subsection. GCs are connected, via some WAN (e.g. Internet), to NOC at the utility provider.

A house h in neighbourhood n has $I_{h,n}$ SDDs and $J_{h,n}$ SDSs, denoted as $SDD_{i,h,n}(i = 1, ..., I_{h,n})$ and $SDS_{j,h,n}(j = 1, .., J_{h,n})$, respectively. This effectively forms the HAN.

All notations used in the paper appear in Table II.

C. Security Attacks and Threat Model

Below we briefly describe the major types of attacks on SG and our considered threat model.

Replay attack: The attacker re-sends a valid and authenticated message in order to waste energy at the receiver or to cause delay. This attack is possible if the message or its digital signature does not contain a timestamp.

Black hole attack: The attacker aims at reducing the amount of data available to legitimate users. This can be achieved by dropping the received messages, instead of sending them further according to the protocol requirements. Furthermore, the attacker may influence the routing table of other nodes, so that the traffic will flow through a compromised node.

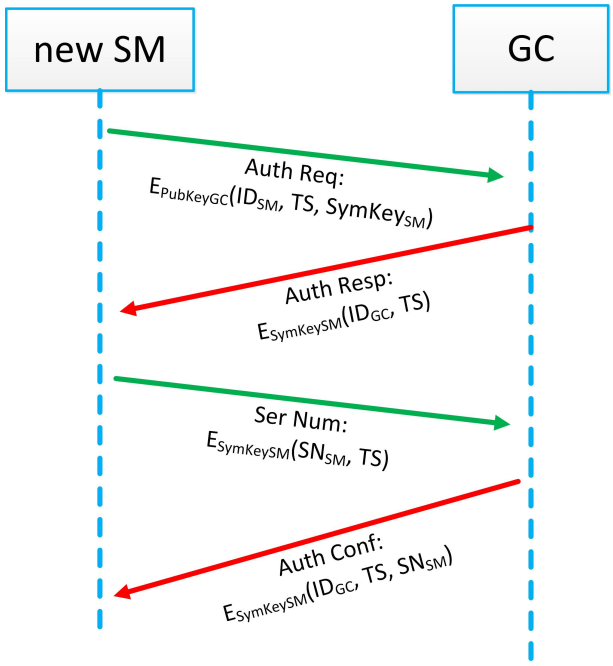

Fig. 2. Direct authentication

Wormhole attack: The attacker receives the packet at one point in the network, sends it to another point, and then replays the packet from that point.

Threat model: As it was mentioned before, some SMs may be used to relay messages from other SMs to GC and vice versa. We assume that some SMs may be compromised and take this into account in the design of our multicast routing protocol. In particular, we design a secure protocol to mitigate against the three aforementioned types of attacks. We assume that GCs and SDs are not compromised.

IV. SECURE MULTICAST ROUTING PROTOCOL

A. Assumptions

We make the following assumptions:

- A SM may need to communicate with GC via other SMs, which may be compromised. Therefore mutual authentication between SM and GC is anticipated.
- All SMs are registered with their associated GC.
- GC is responsible for multicasting and is an aggregator and router for communication with other groups. Furthermore, because of the secure routing issues between GC and NOC, we assume that they have a longer transmission range compared with an ordinary node.
- We assume that an adversary could eavesdrop on all traffic or replay older messages.
- GC is not compromised.

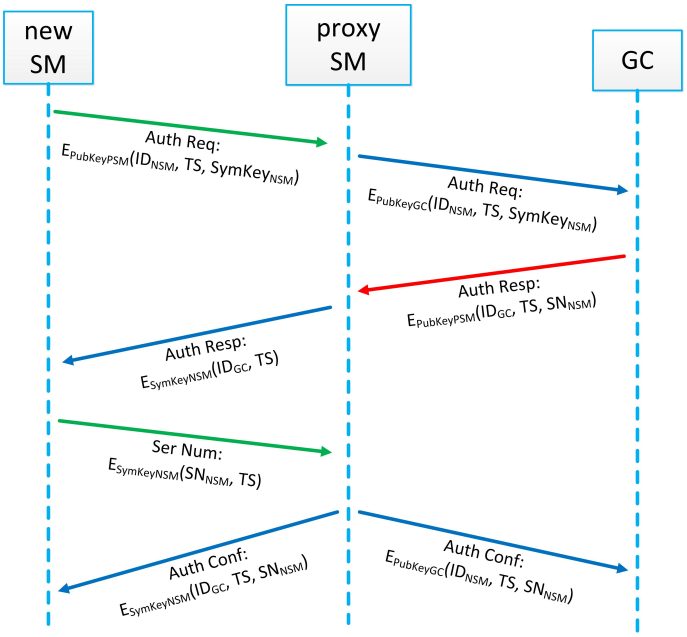

Fig. 3. Indirect authentication

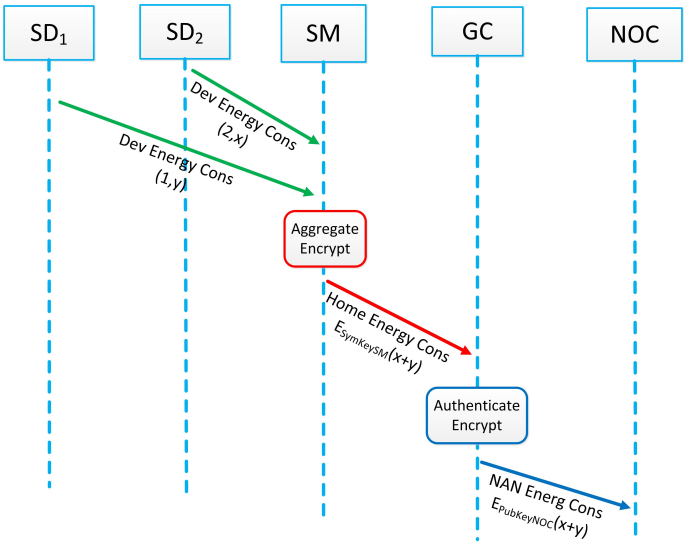

Fig. 4. Reporting energy consumption from HAN to NOC.

- SDs are not compromised.

B. Authentication Phase

GC is responsible for authenticating all SMs belonging to its group. We consider the following two cases:

- Direct authentication: Performed when the new SM has a direct connection with GC.
- Indirect authentication: Performed when the new SM has no direct connection with GC. In that case, the authentication of a *new* SM is facilitated by another, already authenticated SM, referred to as *proxy* SM.

Direct authentication

Initially, the new SM will send the *Authentication Request* message to GC (Fig. 2). This message is encrypted using GC's public key, $E_{PubKeyGC}$, and includes the following information: a) identity number of new SM, ID_{SM}, b) timestamp, TS, c) symmetric key of new SM, $SymKey_{SM}$.

GC responds with the *Authentication Response* message. This message is encrypted using the received $SymKey_{SM}$ and includes the following information: a) identity number of GC, ID_{GC}, b) timestamp, TS.

Next, SM sends its *Serial Number*, SN_{SM}, so that GC may validate this SM as a legitimate one. This message is encrypted using the $SymKey_{SM}$ and includes the following information: a) serial number of new SM, SN_{SM}, b) timestamp, TS.

Finally, GC responds with the *Authentication Confirmation* message. This message is encrypted using the received $SymKey_{SM}$ and includes the following information: a) identity number of GC, ID_{GC}, b) timestamp, TS, c) serial number of new SM, SN_{SM}.

Indirect authentication

Initially, the new SM will send the *Authentication Request* message to the proxy SM (Fig. 3). This message is encrypted using proxy's public key, $E_{PubKeyPSM}$, and includes the following information: a) identity number of new SM, ID_{NSM}, b) timestamp, TS, c) symmetric key of new SM, $SymKey_{NSM}$.

The proxy SM will decrypt and re-encrypt the message using GC's public key, $E_{PubKeyGC}$, and will send it to GC.

GC responds to proxy SM with the *Authentication Response* message. This message is encrypted using proxy's public key, $E_{PubKeyPSM}$, and includes the following information: a) identity number of GC, ID_{GC}, b) timestamp, TS, c) serial number of new SM, SN_{NSM}.

The proxy SM will decrypt and re-encrypt this message using the previously received $SymKey_{NSM}$ and will send the message to the new SM.

Next, new SM sends its *Serial Number*, SN_{NSM}, so that proxy SM may validate the new SM as a legitimate one. This message is encrypted using $SymKey_{NSM}$ and includes the following information: a) serial number of new SM, SN_{NSM}, b) timestamp, TS.

Finally, if the authentication is successful, the proxy SM responds to both new SM and GC with the *Authentication Confirmation* message. This message is encrypted for new SM using $SymKey_{SM}$ and for GC using $E_{PubKeyGC}$, and includes the following information: a) identity number of GC, ID_{GC}, b) timestamp, TS, c) serial number of new SM, SN_{NSM}.

C. Communication Phase

After the authentication phase is over, SMs may communicate with NOC, via their associated GC. We consider the following two communication scenarios, shown also in Figs. 3 and 4.

Reporting energy consumption

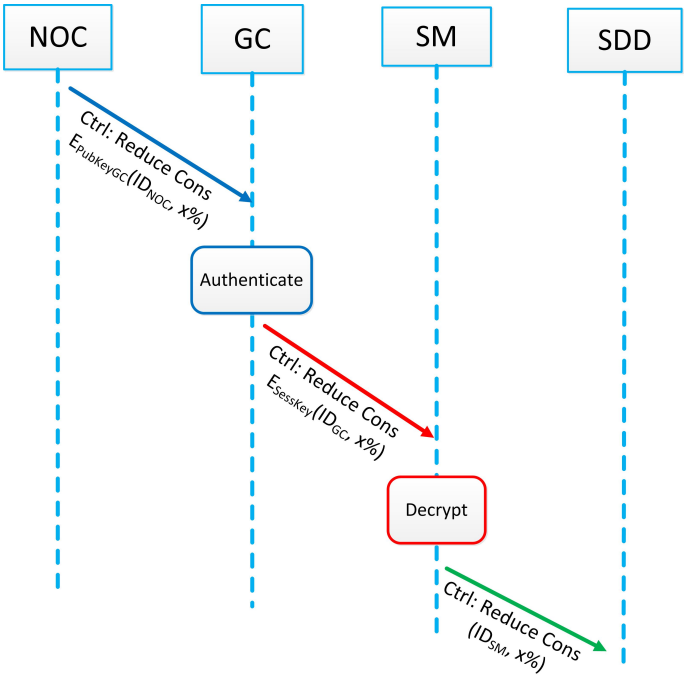

Fig. 5. Sending control message from NOC to HAN.

SDs periodically send their energy consumption to SM. For example, in Fig. 4, SD_1 reports y Joules and SD_2 reports x Joules.

Next, SM aggregates the received consumption data (i.e., $x+y$) from all SDs, encrypts the message using its symmetric key, $SymKey_{SM}$, and sends to GC. Recall that, after the authentication phase, GC knows the symmetric keys of all SMs in its group.

Finally, GC, after having authenticated this message, re-encrypts it with NOC's public key, $E_{PubKeyNOC}$ and sends to NOC.

Sending control messages

From time to time, NOC sends various control messages to GCs and eventually to SMs. For example, in Fig. 5, NOC sends the *Reduce Consumption* message with suggested reduction of $x\%$. This could be the case when the energy consumption is too high or during peak-hours. NOC encrypts this message using GC's public key, $E_{PubKeyGC}$.

GC, after authenticating NOC, will multicast the received control message to all SMs. In order to support multicast, GC will use a session key that is shared among all SMs, $E_{SessKey}$.

Finally, SMs decrypt the control message and forward it to SDDs (recall that SDSs are not able to receive messages).

V. Performance Evaluation

In this section, we evaluate the performance of the proposed multicast routing protocol in terms of energy-efficiency. To this end, we simulate the proposed protocol in NS-3 [25].

A. Simulation Setup

We simulate a SG network consisting of a) one NOC connected to one GC b) GC is connected to 10 SMs, which are inter-connected in a random mesh topology c) each SM is connected to 6 SDs (3 SDDs and 3 SDSs). Recall that the former are able to both receive and send data, whereas the latter are able only to send data. SDs are placed at fixed random locations inside the house and communicate with SM using IEEE 802.15.4 and data transfer rates of 200 Kbps. SMs communicate with each other and with GC using IEEE 802.16 (WiMax) and data rates of 10 Mbps.

SDs generate energy consumption data at periodic intervals of 15 min (similarly to [26]) and of varying sizes 50-500 bytes (according to [27]). These consumption data are aggregated at corresponding SM and are sent to NOC via GC, as described in Section IV. Also, NOC at random time intervals sends control messages. These messages are initially received at GC and then multicasted to SMs. Finally, SMs forward these messages to SDDs.

B. Results-Discussion

Initially, we evaluate the average device energy consumption. In Fig. 6, we present the results for both SDDs and SDSs.

The results show that for small packet sizes (50-150 bytes) the average energy consumption of both SDDs and SDSs is approximately the same. For larger packet sizes, SDDs consume more energy in comparison with SDSs. This is due to the fact, that SDDs not only send data but also receive data from SM. We also observe that when increasing the packet size 10 times (from 50 to 500 bytes), the energy consumption increases very little: approximately 6% for SDDs and by 2% for SDSs.

Next, we evaluate the average traffic demands of the proposed multicast protocol. To this end, we compare the traffic reduction of the multicast mode as compared with the unicast mode. The results of Fig. 7 show that for small packets of 50 bytes, the multicast mode sends approximately 80% (74%) of the traffic in unicast mode for SDDs (SDSs). However, as the packet size increases to 500 bytes, the traffic reduction becomes more significant: 47% for SDDs and 36% for SDSs. We also observe that the traffic reduction is higher for SDSs. This is due to the fact that the multicast mode can be used only for the communication from SM to devices, but not from devices (i.e. SDDs) to SM.

VI. Conclusion

In this paper, we have presented a novel multicast protocol for smart grids. The proposed protocol is both sufficiently secure and energy-efficient, as confirmed by simulation studies. In particular, we prevent some potentially compromised smart meters from issuing a number of security attacks, such as replay, black hole, and wormhole attacks. To this end, we introduce a new entity, called group controller, that acts as security associate. This entity is responsible for authenticating a group of smart meters and for key management. In cases where a smart meter is not directly connected to the group controller, we use indirect authentication which uses a previously authenticated proxy. In our future work, we plan to investigate the cooperation of multiple group controllers, from the security viewpoint.

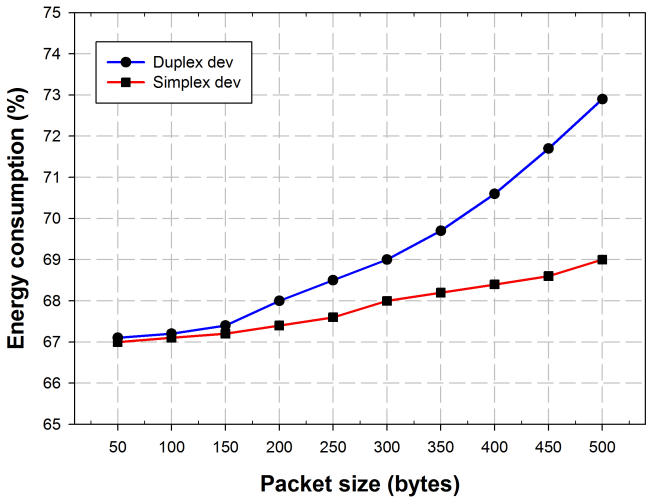

Fig. 6. Energy consumption vs packet size.

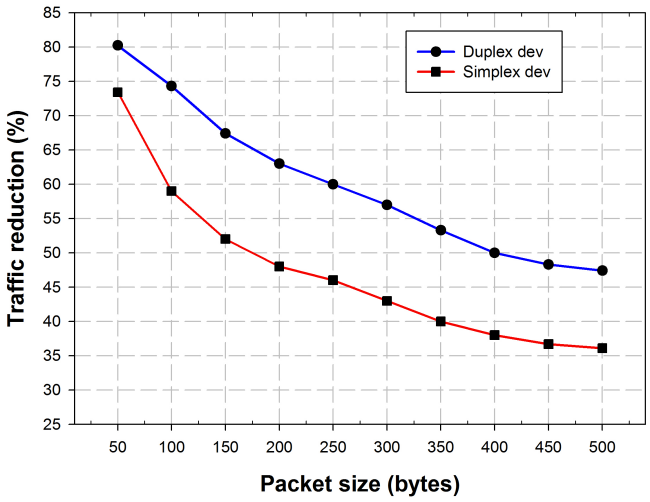

Fig. 7. Traffic reduction vs packet size.

REFERENCES

[1] M. Amin and B. F. Wollenberg, "Toward a smart grid: Power delivery for the 21st century," IEEE Power Energy Mag., vol. 4, no. 6, pp.34-41, Nov. 2006.

[2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid - the new and improved power grid: A survey," IEEE Commun. Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, 2012.

[3] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security & Privacy, vol. 7, no. 3, 75-77, 2009.

[4] X. Li, X. Liang, R. Lu, X. Lin, H. Zhu, and X. Shen, "Securing smart grid: Cyber attacks, countermeasures and challenges," IEEE Commun. Mag., vol. 50, no. 8, pp. 38-45, 2012.

[5] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, W. Chin, "Smart grid communications: overview of research challenges, solutions, and standardization activities," IEEE Commun. Surveys & Tutorials, vol. 15, no. 1, pp. 21-38, 2012.

[6] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," Computer Networks, vol. 56, no. 11, pp. 2742-2771, July 2012.

[7] H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," IEEE J. Sel. Areas Commun., vol. 30, no. 6, pp. 1097-1107, July 2012.

[8] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, G. P. Hancke, "A survey on smart grid potential applications and communication requirements," IEEE Trans. Ind. Inf., vol. 9, no. 1, pp. 28-42, Feb. 2013.

[9] J. S. Vardakas, N. Zorba, and C. V. Verikoukis, "A Survey on Demand Response Programs in Smart Grids: Pricing Methods and Optimization Algorithms," IEEE Commun. Surveys& Tutorials (in press), doi: 10.1109/COMST.2014.2341586

[10] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, vol. 57, no. 5, pp 1344-1371, April 2013.

[11] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, E. Heine, "Design principles for power grid cyber-infrastructure authentication protocols," Proc. 43 Annual Hawaii International Conference on System Sciences (HICSS), 2010.

[12] J.-Y. Kim and H.-K. Choi, "An efficient and versatile key management protocol for secure smart grid communications," Proc. IEEE Wireless Communications and Networking Conference (WCNC), pp. 1823-1828, 2012.

[13] F. Li, B. Luo, and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," 1st IEEE Intl. Conf. Smart Grid Commun., Gaithersburg, MD, USA, pp. 32732, Oct. 2010.

[14] D. Wu and C. Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid," IEEE Transactions on Smart Grid, vol. 2, no. 2, pp. 375-381, June 2011.

[15] H. Nicanfar, P. Jokar, and V. C. M. Leung, "Smart grid authentication and key management for unicast and multicast communications," Proc. IEEE PES Innovative Smart Grid Technologies Asia (ISGT), pp. 1-8, 2011.

[16] S. Das, Y. Ohba, M. Kanda, D. Famolari, and S. K. Das, "A key management framework for AMI networks in smart grid," IEEE Comm. Mag., vol. 50, no. 8, pp. 30-37, 2012.

[17] L. Yee Wei, M. Palaniswami, G. Kounga, and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," IEEE Comm. Mag., vol. 51, no.1, pp. 34-41, 2013.

[18] Q. Li and G. Cao, "Multicast authentication in the smart grid with onetime signature," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 686-696, 2012.

[19] B. E. Bilgin and V. C. Gungor, "Performance evaluations of ZigBee in different smart grid environments," Computer Networks, vol. 56, no. 8, pp. 2196-2205, May 2012.

[20] C.-W. Lu, S.-C. Li, and Q. Wu, "Interconnecting ZigBee and 6LoWPAN wireless sensor networks for smart grid applications," Proc. IEEE Int. Conf. Sensing Technol., pp. 267-272, Dec. 2011.

[21] M. Conti, D. Fedeli, M. Virgulti, "B4V2G: Bluetooth for electric vehicle to smart grid connection," Proc. 9th Workshop on Intelligent Solutions in Embedded Systems (WISES), pp.13-18, July 2011.

[22] W. Meng, R. Ma, and H.-H. Chen, "Smart Grid Neighborhood Area Networks - A Survey," IEEE Network, vol. 28, no. 1, pp. 24-32, 2014.

[23] A. St Leger, J. James, and D. Frederick, "Smart grid modeling approach for wide area control applications," Proc. IEEE Power and Energy Society General Meeting, pp. 1-5, 2012.

[24] S. M. Amin, "Smart grid security, privacy, and resilient architectures: Opportunities and challenges," Proc. IEEE Power and Energy Society General Meeting, pp. 1-2, 2012.

[25] Network Simulator NS-3, http://www.nsnam.com [Dec. 2014].

[26] R. R. Mohassel, A. S. Fung, F. Mohammadi, and K. Raahemifar, "A survey on advanced metering infrastructure and its application in Smart Grids," Proc. IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1-8, 2014.

[27] M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "A Lightweight Message Authentication Scheme for Smart Grid Communications," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675-685, 2011.