An Early Warning System against Malicious Activities for Smart Grid Communications

---

Citation:

Zubair Md. Fadlullah, Mostafa M. Fouda, Xuemin (Sherman) Shen, Yousuke Nozaki, and Nei Kato, "An Early Warning System against Malicious Activities for Smart Grid Communications," IEEE Network Magazine, vol. 25, no. 5, pp. 50-55, Sep.-Oct. 2011.

URL:

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6033036

An Early Warning System Against Malicious Activities for Smart Grid Communications

Zubair Md. Fadlullah, *Member, IEEE,* Mostafa M. Fouda, *Member, IEEE,*
Xuemin (Sherman) Shen, *Fellow, IEEE,* Yousuke Nozaki, *Member, IEEE,* and Nei Kato, *Senior Member, IEEE.*

***Abstract*—Smart grid (SG) presents the largest growth potential in the Machine-to-Machine (M2M) market today. Spurred by the recent advances in the M2M technologies, the smart meters/sensors used in smart grid are expected not to require human intervention in characterizing power requirements and energy distribution. These numerous sensors are able to report back the information such as power consumption and other monitoring signals. However, SG, as it comprises an energy control and distribution system, requires fast response to malicious events such as Distributed Denial of Service (DDoS) attacks against smart meters. In this article, we model the malicious and/or abnormal events, which may compromise the security and privacy of smart grid users, as a Gaussian process. Based on this model, a novel early warning system is proposed for anticipating malicious events in the SG network. With the warning system, SG control center can forecast such malicious events, thereby enabling SG to react beforehand and mitigate the possible impact of the malicious activity. We verify the effectiveness of the proposed early warning system through computer-based simulations.**

***Index Terms*—Smart Grid, Early Warning System, Machine-to-Machine (M2M) communication.**

I. Introduction

THERE is a high expectation recently on the Machine-to-Machine (M2M) communications over wired and wireless links. Various applications of M2M have already started to emerge in various sectors such as healthcare, vehicular ad hoc networks, smart home technologies, and so on [1]. The evolution of M2M has also begun in developing a smart power grid framework, referred to as the smart grid (SG) [2], [3]. An electric grid having smart or intelligent capability allows the power providers, distributors, and consumers to maintain a near real-time awareness of their respective operating requirements and capabilities. Through this awareness, smart grid is able to produce, distribute, and consume power in the most effective manner. This type of communication takes place only amongst machines such as sensors, smart meters, and other equipments. Therefore, the M2M communications in smart grid require to be private and secure since many of the autonomic functions that will run over it will be critical. Smart grid is usually portrayed to have numerous electrical appliances connected with one another in a complex manner so that they can report back on information such as power consumption and other monitoring signals. This promises higher efficiency in the power distribution networks (i.e., greater availability of power to homes and factories at lower cost), and will allow distributed power generation such as local solar and wind generators. It will reach into home-based devices, and therefore, in addition to scalability and fast communication, serious attention should be paid towards smart grid security [4]. Since smart grid communication is going to be based on current networking technologies, the same security concerns often encountered in conventional networks will also be prevalent in smart grid. In fact, cyber threats such as Distributed Denial of Service (DDoS) attacks are likely to have more impact on smart grid communication because of the involvement of so many electrical equipments on the consumer side. By means of early forecasting of malicious threats to smart grid, it may be possible to take quick measure to protect the appliances from being compromised by the attacker. To establish such a forecasting framework, however, we need to consider the fact that humans are not supposed to interfere with M2M communication. Instead, the machines within the smart grid should have an adequate framework to predict or warn about malicious events, abnormality, and failures *a priori*. The machines in the smart grid can be found in different types of networks, such as home-network, building network, and the neighborhood-wide network. The smart meters deployed in these different networks may be utilized to form an information sharing network. Such an information sharing can provide an important resource for developing global and timely assessments of emerging malicious threats against smart grid communication.

While smart meters should authenticate other smart meters and devices, the authentication scheme itself can be targeted by DDoS attackers. In this article, we consider the spread of worm in the smart grid that compromises a number of machines (i.e., smart meters, electrical appliances), which start sending malicious authentication requests to victim smart meters. Such cases observed in a smart grid network are notified to its hierarchically above network, which in turn conveys the information to the smart grid control center. By modeling the malicious attack event through a Gaussian process, the control center can forecast occurrence of future events in the smart grid networks.

The remainder of the article is organized as follows. Section II presents related work in early prediction of network threats. Section III describes the considered architecture for SG communications. Section IV provides our considered DDoS attack model. Section V explains the Gaussian process based proposed scheme for forecasting malicious attacks and Section VI evaluates its performance. Finally, the article is concluded in Section VII.

Z. M. Fadlullah, M. M. Fouda, and N. Kato are with the Graduate School of Information Sciences, Tohoku University, Sendai, Japan. Emails: {zubair, mfouda, kato}@it.ecei.tohoku.ac.jp

X. Shen is with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada. Email: xshen@bbcr.uwaterloo.ca

Y. Nozaki is with NTT Energy and Environment Systems Laboratories, Tokyo, Japan. Email: nozaki.yousuke@lab.ntt.co.jp

II. Related Research Work

Recently, the science of prediction has been ported to SmartGrid research field. It has been revealed that accurate real-time load forecasting is essential for reliable as well as efficient operation of a power system [5]. This work utilizes the accurate reporting of the emerging Advanced Metering Infrastructure (AMI) to track the incoming load requests from Plug-in Hybrid Electric Vehicles (PHEVs). It shows the benefits of the smart use of AMI data in generation planning and load forecasting. Also, Wang *et al.* introduce a data forecasting scheme for determining the electricity consumption *a priori* [6]. This scheme uses three-point Gaussian quadrature approach to construct the forecasting model. A similar approach for predicting power use has also been developed in [7]. This work introduces an extension of kernel regression based on local models which is mentioned to be appropriate for large-scale data mining scenarios in smart grid. A detailed survey is presented in the work by Alfares *et al.* that demonstrates the application of different techniques to forecast loads in power grids [8]. The surveyed approaches consist of multiple regression, exponential smoothing, iterative re-weighted least-squares, stochastic time series, and so on. The survey also highlights the trend that hybrid mechanisms are required to forecast events in power grid that combine two or more of these techniques.

Note that the afore-mentioned works works only consider the smart grid power consumption information and do not investigate whether such models can be effectively employed for forecasting abnormal events in the smart grid power distribution and/or communication networks. Although Gaussian processes have been considered in many learning scenarios in literature [9], they have not been utilized in learning abnormal modes of operation in smart grid. In this article, we simplify the modeling of Gaussian process in smart grid communication for predicting malicious events, which may disrupt the smart meters.

III. Smart Grid Communication Architecture

This section covers the basics of smart grid communication architecture. The smart grid power transmission and distribution system delivers power from the power plant to end-users through a transmission substation and a number of distribution substations. The transmission substation delivers power from the power plant over high voltage transmission lines (generally over 230 kilo volts) to distribution substations, which are placed in different regions. Distribution substations are responsible for converting the electric power into medium voltage levels, and distributing this medium-voltage level power to the building-feeders. To make it usable by the consumers, the building feeders have to convert the medium voltage level into a lower level.

Our considered smart grid communication system is separated from the power transmission and distribution system, and can be viewed as an information sharing network comprising a number of hierarchical components as illustrated in Fig. 1. For communication, however, the above consideration may not be applicable since the communication links have different requirements than those of the power lines. The transmission substation and the control centers of the distribution substations are connected with one another in a meshed network, which can be built over optical fiber technology. The remaining components of the considered SG communication topology is divided into a number of networks, which feature real-life set-ups of a city or a metropolitan area. Broadly speaking, a city has a number of regions (e.g., wards), each of which is covered by a distribution substation. Every region comprises several neighborhoods, each neighborhood has many buildings, and each building may have a number of apartments. We derive our smart grid communication architecture from this real-life planning of a metropolitan area as follows.

The communication architecture for the lower distribution network (beneath the control center) is divided into a number of hierarchical networks, namely Neighborhood Area Network (NAN), Building Area Network (BAN), and Home Area Network (HAN). This is, in spirit, similar to the smart grid system model and processes described in the work by Niyato *et al.* [10]. Each NAN can be considered to be composed of a number of BANs. On the other hand, every BAN contains a number of apartments. The apartments have their respective local area networks, each of which is referred to as a HAN. In addition, there are advanced meters called smart meters deployed in the smart grid architecture that represent AMI for enabling an automated, two-way communication between the utility meter and the utility provider. The smart meters are equipped with two interfaces: (i) power reading interface and (ii) communication gateway interface. The smart meters used in NAN, BAN, and HAN are referred to as NAN GW (GateWay), BAN GW, and HAN GW, respectively. In addition, it is also worth mentioning that based upon the existing standards of smart grid, Internet Protocol (IP)-based communication is preferred to allow virtually effortless interconnections with HANs, BANs and NANs.

A. Neighborhood Area Network – NAN

A NAN is a localized network of the considered SG communication topology. A NAN comprises one or more 3G (Third Generation) base stations and a number of BANs. Notice that the 3G framework used for smart grid communications should be different from the existing ones used for providing other services, e.g., Internet. This should be done in order to prevent network congestion. Also, it is possible to avoid security threats arising from the Internet that may have impact on the delay-sensitive SG communications. It should be noted also that other modes of communications apart from 3G may be alternative solutions for this purpose. The NAN GW can monitor how much power is being distributed to a particular neighborhood by the corresponding control center at the distribution substation.

B. Building Area Network – BAN

Every building connected to the smart power grid maintains its own BAN. A BAN consists of a number of apartments having HANs. The BAN smart meter/GW is typically set up at the building's power feeder. The BAN GW can be used

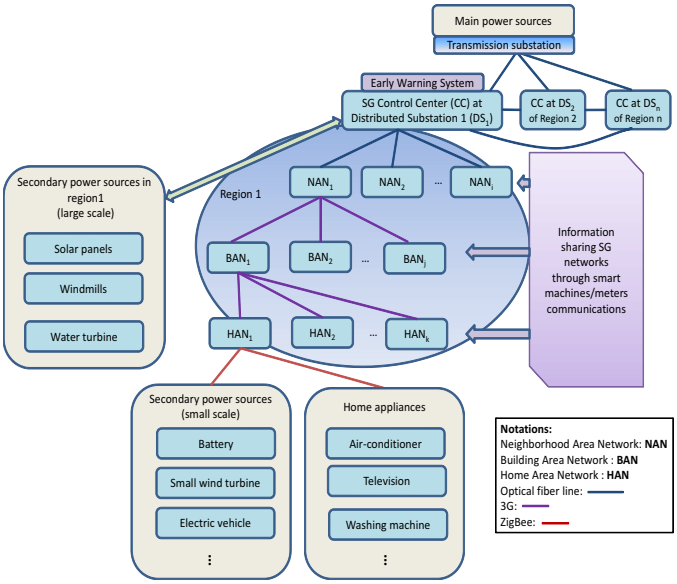

Fig. 1. Smart grid hierarchical networks.

to monitor the power needed and usage of the residents of the corresponding building. In order to facilitate BAN-HANs communication, 3G base stations may be used to cover more areas.

C. Home Area Network – HAN

A HAN is a subsystem within the smart grid dedicated to effectively manage the on-demand power requirements of the end-users. For example, $HAN1$ in Fig. 1 is responsible for the equipments (such as television, washing machine, oven, and so forth) in the first apartment of the considered building to a HAN GW, which, in turn, communicates with $BAN1$. It is worth noting that a HAN can also consist of renewable and/or backup power sources including electrical vehicle, solar panel, battery storage, small wind turbine, and so forth.

IV. Considered Attack Model

The attack model proposed in this section is based on the concept provided in [11] for mitigating Denial of Service (DoS) attacks against broadcast authentication in wireless sensor networks. In our considered attack model, initially an attacker can eavesdrop, inject, and modify packets transmitted in the smart grid network. Also, the attacker has access to at least a smart meter (e.g., a HAN GW) through which he/she infects the network by running computationally resourceful nodes, e.g., laptops and workstations. In addition, the attacker may also use multiple smart meters to launch distributed attacks concurrently. In particular, through worm infection attacks, the attacker may exploit already compromised multiple colluding smart meters in different hierarchical networks of the smart grid. However, we consider that the infected smart meters cannot compromise the cryptographic secrets of other smart meters that are used during authentication.

Authentication is a critical security service in smart grid networks. The authentication mainly involves the smart meters in the different component networks of the smart grid. For example, a HAN GW needs to be authenticated with its corresponding BAN GW before the BAN GW allows it to participate in power demand and response negotiation. Similarly, a BAN GW needs to be authenticated with the NAN GW.

However, the smart meter's authentication scheme may be vulnerable to Distributed Denial of Services or DDoS attacks. For instance, we consider a worm propagation scenario in the smart grid whereby the worm forces the infected host, e.g., a smart meter or some consumer-device, to inject bogus or mal-formed authentication packets to legitimate smart meters. The smart meters at the HAN or BAN are, thus, forced to perform expensive signature verifications to authenticate the compromised hosts. As a consequence, the victim smart meters end up exhausting their already limited memory and processing resources.

In the next section, we propose an early warning system for smart grid to forecast the afore-mentioned DDoS attack.

V. Smart Grid Early Warning System

In this section, first we discuss a set of guidelines for designing an effective early warning system for smart grid. The discussion reveals why Gaussian process regression is chosen for formulating our proposed prediction scheme.

A. Design Guidelines for Smart Grid Early Warning System

The main goal of an early warning system is to reliably predict problems in the smart grid communication network and raise alerts about them. Because smart grid consumers are paying for the service, they expect to get notified quickly about problems emerging in the grid. In particular, the problems, which lead to service interruption or service denial should be detected as soon as possible, even better if they are predicted to the users. For the smart grid control center, early forecasting and warning helps to quickly localize network problems so that they may be fixed more rapidly for providing uninterrupted service to the end-users.

Note that a smart grid network problem can be anywhere, including HANs, BANs, and NANs. The emergence of the problem may be attributed to either communication or power-related issues. In other words, a wide range of problems such as network congestion, power distribution anomalies (e.g., voltage level spikes), malicious attacks, and so on may fall into the scope of prediction. Another design concern of the prediction system should be whether it should be centralized or distributed. While distributed prediction systems may be preferred, we should ask ourselves whether it is practically feasible. Individual smart meters at home or building have limited processing and memory, and therefore, it may not be practical to integrate forecasting feature in these machines. On the other hand, the smart grid control center or the NAN GWs may be equipped with forecasting capability. For example, unusual activities monitored at a building level can be reported to the NAN, and then forwarded to the control center. The control center can, then, predict whether a problem is imminent at the respective smart meter, contact with the smart meter with instructions to take appropriate action to mitigate the problem. In addition, the control center can also issue emergency notifications to building or neighborhood

smart meters, or even other regional control centers, informing them to anticipate a similar abnormal activity.

Finally, the early warning system should not deal with only a single type of malicious activity. However, for clarity and easy explanation, this article sticks with only one malicious case study (i.e., the DDoS attack model described in Section IV). From design point of view, the prediction scheme should be common to different malicious activities to avoid additional complexity due to adoption or combination of different methods. A common architecture for smart grid warning system should be non-parametric, i.e., it should not be affected by the different types of inputs or patterns derived from different malicious activities as mentioned earlier. For example, Gaussian process based models are well established for various spatial and temporal models because Gaussian processes offer a principled, probabilistic approach to facilitate machine learning [12]. In the following, we propose adoption of Gaussian process regression to forecast the malicious activities in smart grid described earlier in Section IV. Gaussian process formulation can also be applied in a similar way to other malicious activities.

B. Gaussian process formulation in smart grid

Consider the notion of random variables to represent abnormal and/or malicious activity features in smart grid communication. Such random variables may be the number of defective smart meters in a building, the fraction of malicious authentication attempts in a given unit of time, and so forth. If we consider such a collection of random variables in smart grid communication, we can formulate a Gaussian process. In this collection of random variables, any finite subset of these variables can be found to have a joint multi-variate Gaussian distribution. Note that a Gaussian distribution is fully specified by a mean vector and a covariance matrix. On the other hand, a Gaussian process is fully represented by a mean function and a covariance or kernel function. Also, note that valid covariance functions lead to positive semi-definite covariance matrices. For two arbitrary inputs to the covariance function, the corresponding functional outputs show the level of similarity.

Gaussian processes offer a rich class of models and when fitted appropriately, they are significantly flexible. One such flexible feature is Gaussian process regression, which we describe next for our forecasting purpose.

C. Gaussian Process Regression

Gaussian process regression is a Bayesian data modeling technique, which fully accounts for uncertainty. Like other Bayesian-based inference approaches, Gaussian processes have a prior and a posterior. Distributions are defined over functions using the Gaussian process which is used as a prior for Bayesian inference. This prior can be flexibly obtained from the training or observation data. In other words, we have prior beliefs about the form of the underlying model. Through observations or experiments, data about the model are obtained. For instance, from smart grid point of view, the data collected from smart meters can be used to form the prior beliefs of a Gaussian process, which characterizes different aspects of the smart grid communication.

Assume that the prior belief about the considered function conforms to a Gaussian process with a prior mean and covariance matrix. Through Gaussian process regression, samples of the function at different locations in the domain are observed. Given a set of observation points and their corresponding real valued observations, it is possible to compute the posterior distribution of a new point. Note that this posterior distribution is also Gaussian, i.e., with mean and variance functions. The optimal parameters of the Gaussian Process are obtained by maximizing the log likelihood of the training data with respect to the parameters. By computing the posterior, it is possible to make predictions for unseen test cases.

D. Covariance function selection

However, to appropriately model the Gaussian process, the choice of the covariance function is important. The reason behind this, as stated earlier, is that it must generate a non-negative definite covariance matrix for any set of points or observations in the smart grid. While stationary and non-stationary covariance functions may be chosen, the choice of a covariance function depends on the problem being solved. In our forecasting approach using Gaussian process regression, we adopt a composite covariance function because it is more flexible in the considered smart grid case that sums covariance contributions from long and short term trends, a periodic component, and fluctuations with various observation lengths. Two isotropic squared exponential covariance functions are used to represent the long and short term trends. The periodic component is the product of a smooth periodic covariance function and another isotropic squared exponential covariance function without latent scale. The fluctuations are represented by an isotropic rational quadratic covariance function.

In the following section, we present the performance evaluation of our proposed forecasting scheme.

VI. Performance Evaluation

To demonstrate the performance of the proposed forecasting scheme, we describe the following scenario comprising the earlier mentioned DDoS attack. In the experimental scenario, we consider a large building having 20 apartments, i.e., the BAN GW is assigned to 20 HAN GWs. The BAN GW is assumed to have ten times higher specification/configuration than that of a HAN GW. Note that the BAN GW is considered to be a smart meter with 160MHz CPU, 128KB RAM, and 1MB flash memory. Now, assume that half of these apartment-owners did not update the firmware of their smart meter devices. As a result, half of the HAN GWs get infected by a worm, which gradually propagates over the considered building area network. The rest of the apartment owners are assumed to have updated their smart meter firmware or operating system with adequate patches. As a result, they are not vulnerable to the worm infection. The HAN GWs, infected by the worm, gradually start to generate malicious authentication requests to the BAN GW at various rates. The BAN GW responds to their authentication requests. The

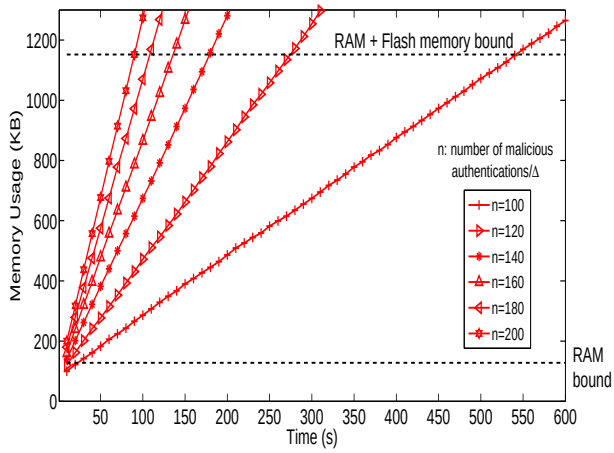

Fig. 2. Memory usage of the victim BAN GW over time for various rates of malicious authentication requests.

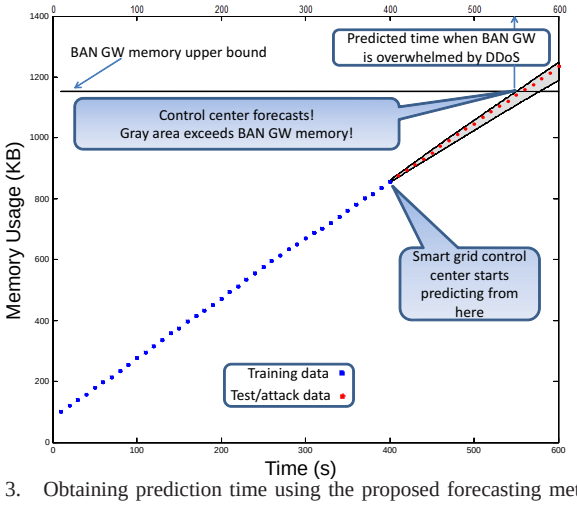

Fig. 3. Obtaining prediction time using the proposed forecasting method.

authentication process is simulated with ECDSA signature verification scheme, which has been already proposed, in existing literature, as an authentication scheme for smart grid communication [13]. Thus, the malicious smart meters attempt at consuming the rather constrained memory resources available at the BAN GW in order to deny legitimate authentication requests from the uninfected HAN GWs.

First, we verify the impact of this simple yet effective attack against the BAN GW through experiments conducted in MATLAB. Fig. 2 demonstrates the memory usage of the victim BAN GW plotted over time for various average rates of malicious authentication requests, denoted by n. In the conducted experiments, the value of n is varied from 100 to 200 per attack launch interval, Δ. The value of Δ was set to a reasonably large value of 10 seconds. Note that n is contributed by the 10 infected HAN GWs during Δ. The results in Fig. 2 demonstrate that the BAN GW memory is fully consumed, i.e., the BAN GW is overwhelmed, more quickly as the value of n increases. For instance, for the lowest considered DDoS attack rate, i.e., $n = 100$, it took 500 seconds to overwhelm the BAN GW memory. On the other hand, for higher values of the attack rate, e.g., $n = 180$ and $n = 200$, it takes just about 80 to 100 seconds to consume the overall memory of the BAN GW. The BAN GW remains busy to verify the malicious authentication signatures, and its limited yet precious memory is consumed while legitimate requests from the remaining uninfected (i.e., legitimate HAN GWs) are turned down. As a consequence, the legitimate smart meters are denied communication with the BAN GW and are unable to specify their power requirements to the smart grid control center.

Next, we present the simulation result of our forecasting algorithm for $n = 100$ as shown in Fig. 3. In this case, a training time of 400 seconds is considered specific to this scenario for $n = 100$ in order to clearly elucidate the way results are obtained in the conducted experiment. The training and test data sets are highlighted in the figure. Notice that the gray area shows the prediction results. The gray area covers the probabilistic predictions, in terms of the projected highest and lowest values of memory usage due to the attack. Also, the average of the highest and lowest values of the gray area corresponds well with the actual test data set. Given this information conveyed from the BAN GW to the NAN GW, the smart grid control center evaluates the forecasting time, and alerts other BAN GWs about possible cyber attacks so that they may take appropriate actions (e.g., ask their respective HAN GWs to update the firmware to prevent worm infection). Also, it is worth noting that for a substantially large training time, the predicted attack occurrence time corresponds with the test data with significant accuracy as shown in Fig. 3.

In Fig. 4, the time instances at which BAN GW memory is predicted to become exhausted, for different values of n, are plotted. It is worth mentioning that the delay of BAN GW to control center communication has not been considered here because it does not change the purpose and the fundamental results of the conducted simulations. The training time considered in Fig. 4 is much lower than that considered in the result shown in Fig. 3. The reason behind this is the fact that higher values of n cause the BAN GW to be overwhelmed by the corresponding DDoS attack fairly quickly. Therefore, the training time is set to 50 seconds, i.e., lower than the actual value of the BAN GW memory exhaustion time (i.e., 80 seconds) for the considered highest DDoS attack rate (i.e., n=200). As evident in Fig. 4, the time taken by the control center to predict the attack occurrence is reasonable. However, the only shortcoming is that the BAN GW memory exhaustion due to the lowest attack rate is not predicted by the control center since it does not manifest enough attack features during the short time period. Therefore, it is also important to adopt different windows of training time simultaneously to catch the effect of both the moderate and high rates of DDoS attacks.

VII. Conclusion

In this article, we have presented a framework for forecasting malicious attacks, which may arise in emerging smart power grids. The framework uses probabilistic distribution to predict if some abnormal mode of operation is going to disrupt smart grid communications. Simulation results demonstrate that the proposed scheme can warn the malicious DDoS attacks beforehand. In addition to the described attack in this article, other malicious threats and anomalies (e.g., abnormal voltage surges and fluctuations) may also be predicted using

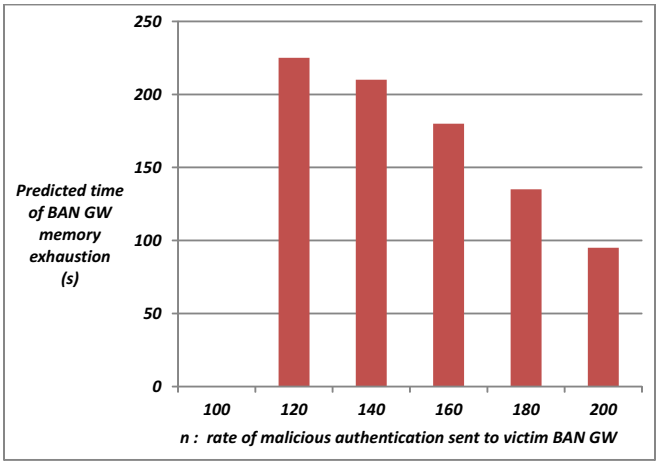

Fig. 4. Predicted time of BAN GW memory exhaustion by the proposed algorithm for shorter training time of 50 seconds in case of different DDoS attack rates.

the proposed scheme so that the control center can instruct smart meters to take actions against such anomalies promptly. However, for actual networks in the smart grid with background traffic, we need to establish a baseline for estimation errors in identifying actual abnormal activities. These issues will comprise our future study.

REFERENCES

[1] R. Lu, X. Li, X. Lin, X. Liang, and X. Shen, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 28–35, Apr. 2011.

[2] C. W. Gellings, "The Smart Grid: Enabling Energy Efficiency and Demand Response," published by CRC Press, Aug. 2009.

[3] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Towards intelligent machine-to-machine communications in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 60–65, Apr. 2011.

[4] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid*, 2011, to appear.

[5] M. Alizadeh, A. Scaglione, and Z. Wang, "On the impact of smartgrid metering infrastructure on load forecasting," in *Invited article in Proc. 48^{th} Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, Sept. 2010.

[6] X. Wang, H. Wang, and L. Hou, "Electricity demand forecasting based on threepoint gaussian quadrature and its application in smart grid," in *Proc. 6^{th} Int. Wireless Communications Networking and Mobile Computing (WiCOM) Conf.*, Chengdu, China, Sep. 2010, pp. 1–4.

[7] O. Kramer, B. Satzger, and J. Laessig, "Power prediction in smart grids with evolutionary local kernel regression," in *Proc. Hybrid Artificial Intelligence Systems (HAIS'10)*, San Sebastian, Spain, Jun. 2010.

[8] H. K. Alfares and M. Nazeeruddin, "Electric load forecasting: literature survey and classification of methods," *International Journal of Systems Science*, vol. 33, no. 1, pp. 23–34, Dec. 2001.

[9] T. I. Alecu, S. Voloshynovskiy, and T. Pun, "The gaussian transform of distributions: definition, computation and application," vol. 54, no. 8, pp. 2976–2985, Aug. 2006.

[10] D. Niyato, P. Wang, Z. Han, and E. Hossain, "Impact of packet loss on power demand estimation and power supply cost in smart grid," in *IEEE Wireless Communications and Networking Conference (WCNC'11)*, Cancun, Quintana Roo, Mexico, Mar. 2011, pp. 2024–2029.

[11] P. Ning, A. Liu, and W. Du, "Mitigating dos attacks against broadcast authentication in wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 4, no. 1, Feb. 2008, pp. 1–35.

[12] J. Zhang, P. Porras, and J. Ullrich, "Gaussian process learning for cyber-attack early warning," *Stat. Anal. Data Min.*, vol. 3, no. 1, Feb. 2010, pp. 56–68.

[13] M. Kgwadi and T. Kunz, "Securing RDS broadcast messages for smart grid applications," in *Proc. 6^{th} International Wireless Communications and Mobile Computing Conference* (IWCMC'10), Caen, France, Jun. 2010, pp. 1177–1181.

BIOGRAPHIES

Zubair Md. Fadlullah [M'11] (zubair@it.ecei.tohoku.ac.jp) received B.Sc. degree with Honors in computer sciences from the Islamic University of Technology (IUT), Bangladesh, in 2003, and M.S. and Ph.D. degrees from the Graduate School of Information Sciences (GSIS), Tohoku University, Japan, in 2008 and 2011, respectively. Currently, he is serving as an Assistant Professor at GSIS. His research interests are in the areas of smart grid, network security, intrusion detection, and quality of security service provisioning mechanisms.

Mostafa M. Fouda [M'11] (mfouda@it.ecei.tohoku.ac.jp) received B.Sc. degree with Honors in electronics and communications engineering, and M.Sc. degree in electrical communications in 2002 and 2007, respectively, from the Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt. He received his Ph.D. degree from the Graduate School of Information Sciences (GSIS), Tohoku University, Japan, in 2011. Currently, he is serving as as a Postdoctoral Research Fellow at GSIS and also an Assistant Professor at Benha University. His research interests include smart grid communications, network security, peer to peer applications, and multimedia streaming.

Xuemin (Sherman) Shen (xshen@bbcr.uwaterloo.ca) [M'97, SM'02, F'09] received a B.Sc. (1982) degree from Dalian Maritime University, China, and M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey, all in electrical engineering. He is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on mobility and resource management, UWB wireless networks, wireless network security, and vehicular ad hoc and sensor networks. He served as an Area Editor for IEEE Transactions on Wireless Communications and Editor-in-Chief for Peer-to-Peer Networks and Applications. He is a Fellow of Engineering Institute of Canada, a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society.

Yousuke Nozaki [M] (nozaki.yousuke@lab.ntt.co.jp) is a project manager, senior research engineer, supervisor, Energy System Project, NTT Energy and Environment Systems Laboratories. He received B.E. and M.E. degrees in mechanical engineering from Tohoku University, Miyagi, in 1987 and1989, respectively. He joined NTT Laboratories in 1989. Since then he has been engaged in R&D of switching power regulators, photovoltaic and fuel cell power systems, and high-voltage direct current power systems for telecommunications systems. He is a member of IEICE and the Institute of Energy Economics, Japan.

Nei Kato [M'03, A'04, SM'05] (kato@it.ecei.tohoku.ac.jp) has been a full professor at GSIS, Tohoku University, since 2003. He has been engaged in research on computer networking, wireless mobile communications, and smart grid, and has published more than 200 papers in journals and peer-reviewed conference proceedings. He currently serves as Chair of the IEEE Satellite and Space Communications Technical Community (TC) and Secretary of the IEEE Ad Hoc & Sensor Networks TC.