A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure

Xiaoxue Liu, *Student Member, IEEE*, Peidong Zhu, *Senior Member, IEEE*,
Yan Zhang, *Senior Member, IEEE*, and Kan Chen

***Abstract*—Smart meters are inherent components in advanced metering infrastructure (AMI) in the smart power grid. They are serving as the crucial interfaces through which the cyber, physical, and social domains of the smart grid can interact with each other. Due to the complicated interactions, smart meters may face a large variety of threats. In this paper, we exploit the colored Petri net to describe the information flows among units in a smart meter. Then, we propose a threat model for smart meters. Considering the constrained computation and storage resources of a smart meter, we present a collaborative intrusion detection mechanism against false data injection attack. The proposed scheme can work regardless of changes in a smart meter's software. Numerical results demonstrate the low cost and effectiveness of our proposed intrusion detection mechanism.**

***Index Terms*—Advanced metering infrastructure (AMI), collaborative intrusion detection, colored Petri net, smart grid, smart meters, spying domain, threat model.**

I. Introduction

SECURE and efficient advanced metering infrastructure (AMI) is very important for the smart grid [1]–[3] and smart meters are the essential devices to construct AMI networks. Smart meters support two-way communications. On the one hand, smart meters collect users' power consumption data and then transmit the data to utility companies. On the other hand, smart meters can receive information about electricity price and commands from utility companies and then deliver them to users. Smart meters are regarded as the key interfaces for physical, information, and social domains of the smart grid in AMI systems. However, they may suffer from a variety of threats, including both cyber attacks and physical attacks from customers who may tamper with the smart meters to generate lower energy consumption bills. People or software may maliciously disrupt or even destroy the meter reading. Understanding the attacks toward smart meters is a fundamental challenge for constructing a security mechanism.

Petri net and its variations have been powerful tools for studying various types of asynchronous and concurrent processes [4], [5]. McDermott [6] was likely the first one to point out the usefulness of Petri nets for cyber attack modeling and observed that Petri nets are good at capturing concurrent actions of an attack [6]. Dalton *et al.* [7] presented a generalized stochastic Petri net to model and analyze attack trees with the ultimate goal of automating the analysis. Wu *et al.* [8] suggested colored Petri nets for hierarchical attack modeling to describe attacks in two levels, those being generally and specifically. When it comes to the electrical power system, Petri nets have been applied to show interdependencies between the preexisting electrical power and communications infrastructures [9]–[11]. In addition, Calderaro *et al*. [12] presented a Petri net-based method to identify and localize failures in the smart grid. Chen *et al.* [13] proposed a new hierarchical method to construct a large Petri net from a number of small Petri nets for modeling the cyber-physical attacks on the smart grid. It is observed that the aforementioned studies just consider the smart meter as the components of AMI networks and use Petri net to model attacks on smart meters directly. In this paper, we are motivated to capture smart meters behavior and their consequence on potential threats. In this case, we should consider the components and information flows of smart meters as basic units in Petri net-based AMI modeling, which is very different from the existing studies. When Petri net is used to model a specific smart meter, the components of the smart meter are taken into account specifically and finer granularities description is needed so as to capture specific information flows and their occurring conditions.

With respect to the protection strategies for smart meters, we can observe three major techniques: 1) intrusion detection system (IDS); 2) remote attestation technologies; and 3) smart meter software modeling. Berthier and Sanders [14] modeled the communication software of a smart meter and introduced a specification-based IDS which can detect the abnormal communications but cannot verify whether they are attacks. LeMay *et al.* [15] built a remote attestation architecture to ensure the integrity of smart meter software and hardware. Tabrizi and Pattabiraman [16] used state machines to detect the anomalies of software. Faisal *et al.* [17] proposed an IDS architecture for AMI using a data stream mining approach.

Manuscript received May 13, 2014; revised September 18, 2014 and January 18, 2015; accepted March 24, 2015. Date of publication April 16, 2015; date of current version August 19, 2015. This work was supported by the National Natural Science Foundation of China under Grant 61170285. Paper no. TSG-00431-2014.

X. Liu, P. Zhu, and K. Chen are with the School of Computer Science, National University of Defence Technology, Changsha 410073, China (e-mail: xiaoxue@nuaa.edu.cn).

Y. Zhang is with the Department of Informatics, University of Oslo, Oslo 1325, Norway.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2015.2418280

The studies on security mechanism for smart meters have mainly focused on applying the existing networks and software security technologies into smart meters. Few studies have investigated smart meters' physical components. In addition, the limited computation and storage resources of smart meters have not been given full consideration.

In this paper, we aim to build threat models for smart meters and propose new scheme to defend typical attack on smart meters. The main contributions of this paper are presented as follows.

1) We exploit the colored Petri net to model the smart meter architecture and the information flows within a smart meter. Based on this, we then build a threat model to describe specific attacks toward smart meters through analyzing the data and the commands flow in a smart meter.
2) We propose a new concept of spying domain to protect the data in smart meters, which has been shown to be cost-effective.
3) We consider the constrained resources in smart meters and then present a collaborative intrusion detection mechanism against false data injection attack in AMI networks.

The rest of this paper is organized as follows. In Section II, we introduce the physical architecture of a smart meter and use the colored Petri net to depict the information flows within the smart meter. In Section III, threat model is built up through analyzing information flows in a smart meter. In Section IV, we consider the constrained computation and storage resources and propose a low-cost collaborative intrusion detection mechanism. In Section V, we evaluate the performance of the proposed scheme. Finally, we conclude this paper in Section VI.

II. Smart Meter Architecture Based on Petri Net

A. Physical Architecture of Smart Meter

Smart meter's physical architecture is typically composed of sensors, microcontroller, physical memory, network interface, and input buffer [16].

As Fig. 1 shows, sensors collect user data, convert the data from electronic signal to digital data and then pass them to the microcontroller. Based on the input data, the microcontroller calculates user's consumption information. To cope with failures (e.g., blackout and network disconnections), physical memory stores consumption information temporarily and the log file. Smart meters communicate with servers or other devices via network interfaces where data are sent and received. Input buffer is used to received information (e.g., price and commands) from the utility companies.

B. Petri Net and Colored Petri Net

Petri net was originally invented to describe asynchronous and concurrent phenomena [18], [19]. It can describe physical phenomena in an abstract way, interpret the relations between resources and processes, and depict information flows through synchronous and asynchronous elements. Therefore, the Petri net can be applied to depict the asynchronous and concurrent information flows in smart meters.

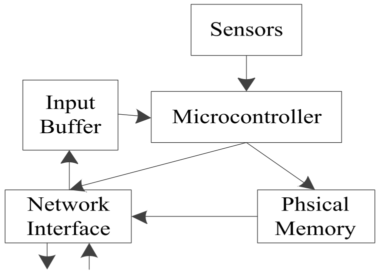

Fig. 1. Physical architecture of a smart meter.

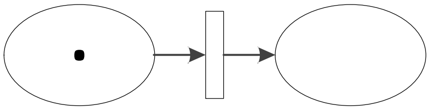

Fig. 2. Petri net.

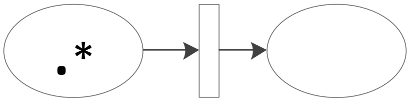

Fig. 3. Colored Petri net.

Fig. 2 shows a Petri net. A Petri net is usually made up of the following elements.

1) *Place:* Circular or elliptical nodes.
2) *Transition:* Rectangular nodes.
3) *Connection:* Directed connection between a place and a transition.
4) *Token:* The black dot, dynamic objects in place which can shift from one place to another.

A Petri net must satisfy the following rules.

1) All connections must be directed.
2) A connection can only be located between a place and a transition and the connections between places or between transitions are not permitted.
3) A place can have one or many tokens.

Several extensions have been made for the basic Petri net [4], [20], [21] and the colored Petri net is one of them. Through the colored Petri net, it is possible to describe data types and complex data manipulations with each token attaching a data value called token color [22]. In this paper, we will use different shapes to represent the colored tokens. Fig. 3 shows that there are two types of tokens, the starred one "$*$" and the dotted one "$\bullet$." For example, we can use the starred tokens and the dotted tokens to represent the user data and the commands from utility companies to smart meters, respectively.

C. Smart Meter Architecture Based on Colored Petri Net

A Petri net model allows the description of simultaneous processes. Since there may be concurrent information flows in a working smart meter, a Petri net is shown to be appropriate to describe those information flows. The information in a smart meter has two types: 1) the collected user data; and

TABLE I
TRANSITIONS IN A SMART METER ARCHITECTURE BASED ON THE COLORED PETRI NET

Transition Number	Information Flow Types	Input Place	Output Place	Occurring Conditions	Specific Processes of Information Flows
1	Data flow	sensors	microcontroller	sensors and microcontroller work normally & legal commands from utilities	microcontroller receiving user data from sensors
2	Data flow	microcontroller	network interface	Available network connection	microcontroller passes consumption data to network interface
3	Data flow	microcontroller	physical memory	Unavailable network connection	microcontroller writes consumption data to physical memory
4	Data flow	physical memory	network interface	Available network connection & legal reading in physical memory	Read data from physical memory to network interface for sending
5	Data flow	AMI Network	network interface	Available network connection	network interface receives data from utility companies or other devices
6	Commands flow	AMI Network	network interface	Available network connection	network interface receives commands from utility companies or other devices
7	Data flow	network interface	input buffer	Available network connection	Data from utility companies or other devices are put into input buffer
8	Commands flow	network interface	input buffer	Available network connection	Commands from utility companies or other devices are put into input buffer
9	Commands flow	input buffer	microcontroller	Commands are verified legal	Commands are passed from input buffer to microcontroller to be executed
10	Data flow	input buffer	network interface	Available network connection	Data from other devices are passed back to network interface for forwarding
11	Data flow	network interface	AMI Network	Available network connection	Consumption data is sent via network interface

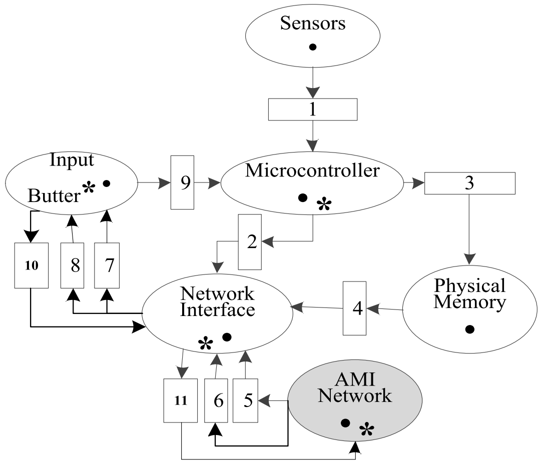

Fig. 4. Smart meter architecture based on the colored Petri net.

2) the commands from utility companies. Thus, we use the colored Petri net to describe different information flows among a smart meter's components.

Fig. 4 shows the smart meter architecture based on the colored Petri net. The elliptical domains (i.e., places), tokens and rectangular domains (i.e., transition) represent a smart meter's components, information, and information interactions among components, respectively. There are two types of tokens, the dotted tokens "•" represent user data and the starred tokens "∗" represent commands from utility companies. A directed connection represents information flow's direction when a transition occurs. The place "AMI network" representing communication networks is also set to achieve a complete description of information flows in a smart meter. Transitions 5, 6, and 11 show information interactions between a smart meter and AMI networks.

From the colored Petri net-based smart meter architecture, we can conclude that the occurrence of a transition will bring out information flows between two components of the smart meter. To depict the information flows in detail, we define the transition for smart meters as

Transition:
<
Transition Number, Information Flow Type,
Input Place, Output Place, Occurring Condition,
Specific Process of Information Flow
>.

Table I summarizes the process and occurring conditions of each information flow in a smart meter. We have classified the information flows in a smart meter into two types: 1) the data flow; and 2) the commands flow. The data consists of the consumption information of users and the electricity price from the utility companies. The commands usually include the reading, forwarding, or disconnecting commands from the utility companies or other devices. There are data and commands in the input buffer. However, only the commands in the input buffer will be passed to the microcontroller for execution and data from other devices in the input buffer will not be passed to the microcontroller so as to avoid repeated computation. Hence, transition 9 represents the commands flow: the commands are passed from the input buffer to the microcontroller for execution. Transition 10 represents data flows: data from other devices is passed back to the network interface to be sent.

III. THREAT MODELS

Existing studies mainly focus on threats and security requirements of the smart grid and AMI [23]–[34]. In [35], threats toward AMI networks are classified in terms of attackers, attack motivations, and attack techniques. In [36], threats

TABLE II
THREAT MODEL FOR SMART METERS

Attack Types		Attacks on data	Attacks on commands
Targeted Information Flows		Transitions 1, 2, 3, 4, 5, 7, 10, 11	Transitions 6, 8, 9
Occurring Locations		All smart meter's components and interacting processes of the data among them;	More likely to occur at the network interface, input buffer and microcontroller of a smart meter;
Attack Techni-ques	**Physical attack**	1) Physically break smart meters' components so as to destroy the normal process of data collecting, computing, storing and transmitting. 2) Physically disconnect smart meters; 3) Physically extract secret keys from smart meters. 4) Reverse the smart meters [37]**;**	1) Physically break the input buffer or network interface to prevent legitimate commands being received; 2) Physically break the microcontroller to prevent commands being executed; 3) Physically extract secret keys from smart meters. 4) Physically disconnect smart meters; 5) Abuse optical ports to gain access to smart meters [37].
	Cyber attack	1) Compromise smart meters or steal credentials through remote network exploitation; 2) Tamper with and even delete consumption data in physical memory by injecting malicious codes or false data; 3) Eavesdroping the outgoing/incoming traffic via network interface to analyze users' private habits; 4) Filling input buffer with dummy data so that the legitimate data from other devices can not be accepted; 5) Flooding network bandwidth to cause network connection unavailable.	1) Steal credentials through remote network exploit to isolate the encryption and authentication mechanism; 2) Sending counterfeit commands to smart meters, such as disconnect the smart meter illegally; 3) Filling input buffer with spam data so that the legitimate commands are rejected. 4) Flooding network bandwidth to cause network connection unavailable.

are categorized into three types: 1) network compromise; 2) system compromise; and 3) denial of service and they are described from the perspectives of attack techniques and attack consequences. Grochocki *et al.* [37] presented an extensive survey of AMI-specific threats and a detailed mapping to the information required for accurate attack detection. These work are performed mainly from the cyber security perspective. In addition, the existing works mainly focused on a high-level classification of possible malicious activities toward smart meters. A specific threat model on smart meters needs further investigation. As integrated interfaces for the physical and cyber domains of the smart grid, smart meters face threats from both physical attacks and network attacks. For example, motivated by financial benefits, consumers may tamper with the consumption data in a smart meter in order to reduce their charges for electricity or increase the generation amount.

The ultimate objective of smart meter protection is to ensure the information security [38]. We analyze threats on information flows in a smart meter in Table I and obtain attacks' occurring locations and attacking techniques according to the colored Petri net-based smart meter architecture. Since information flows in a smart meter comprise both data and commands, this section categorizes the attacks toward smart meters into attacks on data and attacks on commands.

Table II shows the threat model for smart meters. Attackers are likely to use multiple attack means by the same time. For instance, they may firstly disconnect a smart meter by flooding its network bandwidth to make the network connection unavailable, which can cause occurrence of transition 3 (consumption data is written to physical memory) in Fig. 3. Then, consumption data in physical memory can be tampered and even deleted by physical attack or false data injection. Hence, when the communications network is available again, the tampered data or even no data is sent via the network interface.

Physical attacks are usually powerful and efficient while they are also easier to be detected. To resist against physical attacks, smart meters can be strengthened physically and equipped with an alerting system. Once being compromised physically, an alerting signal is sent out. In contrast, cyber attacks toward smart meters may not be easily observed and can also cause serious damages. There have been several security techniques to cope with these cyber attacks. Signature on commands can be used to deal with illegal command attacks. By restricting data receiving rates at the network interface and clearing the input buffer regularly, the input buffer can be protected from being overwhelmed by massive spam data. Encryption can be used to stop eavesdropping on the network interface.

Among all attacks in Table II, a typical attack in real life is to tamper with or even delete legitimate consumption data in the physical memory of a smart meter by injecting malicious codes or false data for the sake of financial benefits [29], [30], [34], [38]. This type of attack is usually called false data injection attack. Although those attack can be achieved through physical means such as reversing or shifting forward the smart meter directly, physical attacks can be easily detected. Cyber attacks tend to be more persistent. Attackers may take the following steps. First, attackers may exhaust the network bandwidth to cause network disconnection and consumption data is written to physical memory (transition 3). Then, attackers inject malicious codes into smart meters which can perform illegal writing or reading operations in physical memory. Therefore, when the network connections become available again, the modified data is sent via network interface.

IV. PROPOSED COLLABORATIVE INTRUSION DETECTION MECHANISM AGAINST FALSE DATA INJECTION ATTACK

In this section, we will propose an efficient intrusion detection mechanism, considering the constrained computation and memory resources of the smart meters. Intrusion detection is the process that monitors the events occurring in a computer system and analyzes the events to find out possible incidents [39]–[41]. Traditional detecting technologies on malicious codes applied to computers are very power-hungry. Our proposed intrusion detection mechanism can achieve collaborative detection of false data injection attack by setting spying domain randomly in physical memory in combination with using secret information and event log. Once the spying domain is modified, illegal reading or writing is identified.

The idea of setting spying domain for intrusion detection is inspired by a tool called "StackGuard" for the buffer overflow attack. StackGuard inserts a spying word called "Canary" between the return address of memory and the buffer. If the Canary is modified, buffer overflow attack is detected [42]. However, there is a fundamental difference between the spying word Canary and the spying domain proposed in this paper: the location of the Canary is fixed while the spying domain is composed of multiple storage units. The storage units are chosen randomly when legitimate reading or writing occurs in the physical memory of the smart meter. The proposed mechanism has the following requirements.

1) *Secret Information:* Each smart meter has its own secret information and only legitimate procedures can access it. The confidentiality of secret information influences the effectiveness of the intrusion detection mechanism. Hence, it should be updated regularly to resist leakage.
2) *Event Log:* Each smart meter has an event log to record all events including processes of parsing and executing commands to calculate consumption data in the microcontroller, reading/writing in the physical memory, and receiving/sending data via the network interface. The event log is encrypted with the secret information.
3) *Spying Domain:* Every time a legal procedure writes consumption data into the physical memory, several discontinuous storage units are chosen randomly as the spying domain. Then, the hash result of secret information will be written into it. Addresses of spying domain are stored in the event log and the spying domain will be cleared after being read legally. The spying domain is essential for the collaborative intrusion detection mechanism because the spying domain's effectiveness and cost determine the performance of the detection mechanism.

A. Definition of Legitimate Writing and Reading

In order to detect illegal operations on physical memory, legitimate writing and reading are defined as follows.

1) Legitimate Writing Operation in Physical Memory: We choose storage units from physical memory randomly as the spying domain and write into it the hash result of the secret information. Then, we write the addresses of the spying domain and the hash result of secret information into the event log. In addition, we encrypt the event log with the secret information. Finally, we write normal consumption data to the physical memory excluding the spying domain.

2) Legitimate Reading Operation in Physical Memory: We first decrypt the event log with secret information to get the addresses of the spying domain and encrypt the event log again. Then, we read normal consumption data from the physical memory while avoiding reading the spying domain.

B. Classification of Attackers

In the context of AMI networks, attackers are categorized into six types according to their motivations [36]. In [44], attacks are viewed as a set of capabilities defined as amounts of information required or the expected situation that must exist for a particular attack to occur.

In this paper, we mainly focus on the unethical consumers who want to steal electricity by tampering with smart meters through false data injection attack. We categorize the attackers according to their attack ability and the attack ability mainly depends on the amount of knowledge that is acquired by attackers about their targets. Attackers are divided into three types.

1) Innocent Attackers: They learn nothing about the architecture and software of a smart meter, and they do not know the existence of IDS including the spying domain, and cannot access the secret information.

2) Skilled Attackers: They have acquired the detailed information about the architecture and software of a smart meter. Thus, they know the existence of IDS and the spying domain. The attackers try to perform legitimate procedures as possible as they can and want to avoid the spying domain when reading or writing the physical memory illegally. However, they cannot obtain the secret information and are unable to decrypt the event log to access the spying domain's addresses.

3) Powerful Attackers: They can obtain detailed information about the software of a smart meter, the existence of spying domain, and also the secret information. They can successfully decrypt the event log to get the addresses of the spying domain and write into the event log. The powerful attackers have access to the physical memory of a smart meter.

C. Illegal Writing and Reading

According to the classification of attackers, illegal reading and writing in the physical memory may take place in several situations.

1) Illegal Writing: In the case when consumption data have been written into the physical memory by legitimate procedures, if the attackers are innocent and skilled ones, malicious codes will write the physical memory blindly and cause the spying domain to be covered. When the attackers are powerful ones, malicious codes will avoid the spying domain to write false data into or modify consumption data in the physical memory.

In the case when consumption data have been read legally and the physical memory is empty, if the attackers are innocent ones, malicious codes will not set the spying domain or operate the event log correctly. When the attackers are skilled ones, they cannot generate the correct hash result of the secret information or operate the event log correctly. When the attackers are powerful ones, malicious codes can set the spying domain and decrypt/encrypt the event log, thus they may write false data into or modify the normal consumption data in the physical memory successfully.

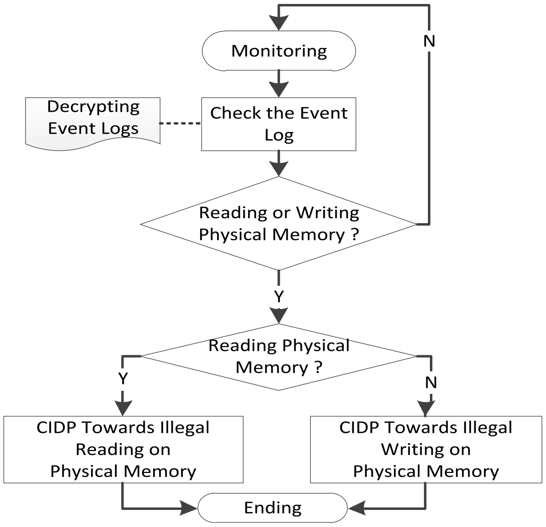
Monitoring
N
Decrypting Event Logs
Check the Event Log
Reading or Writing Physical Memory ?
Y
Reading Physical Memory ?
Y
N
CIDP Towards Illegal Reading on Physical Memory
CIDP Towards Illegal Writing on Physical Memory
Ending

Fig. 5. Collaborative intrusion detection procedure.

2) Illegal Reading: There are two cases for illegal reading. When the attackers are innocent and skilled ones without the secret information, malicious codes will read the physical memory blindly which causes the spying domain to be read and cleared. When the attackers are powerful ones, malicious codes would avoid the spying domain and read consumption data in the physical memory successfully.

D. Collaborative Intrusion Detection Processes

When the attackers are the innocent or skilled ones, malicious codes are not able to set the spying domain or operate the event log. The illegal reading in the physical memory in this case will be easily captured by IDS and an alerting signal will be triggered. When the attackers are powerful ones, it becomes difficult for IDS to detect the illegal operations in the physical memory. On this occasion, the event log should be checked out. These records should be analyzed comprehensively in order to find out the hidden attacks.

Fig. 5 shows the process of the collaborative intrusion detection for a smart meter. The intrusion detection mechanism will examine the event log to judge if the physical memory has been read or written and then start an appropriate detecting procedure.

1) Collaborative Intrusion Detection Procedure Toward Illegal Writing in Physical Memory: When a smart meter receives legitimate reading commands from a utility company, the microcontroller calculates user consumption data based on the information collected by sensors. Then, the network connection will be checked by the network interface. If the network connection is unavailable, user consumption data will be written into the physical memory. Otherwise, user consumption data will be sent via the network interface. Hence, the illegal writing operations in the physical memory comprise the following two scenarios.

1) Writing the physical memory under the condition that a smart meter has not received legal reading commands.
2) Writing the physical memory under the condition that network connection is available and user consumption data should be transmitted.

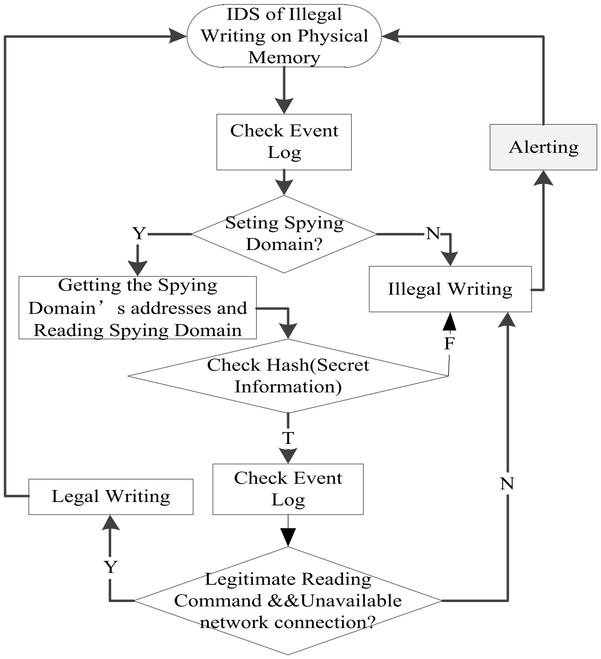
IDS of Illegal Writing on Physical Memory
Check Event Log
Alerting
Seting Spying Domain?
Y
N
Getting the Spying Domain’ s addresses and Reading Spying Domain
Illegal Writing
F
Check Hash(Secret Information)
T
Legal Writing
Check Event Log
N
Y
Legitimate Reading Command &&Unavailable network connection?

Fig. 6. Collaborative intrusion detection procedure toward illegal writing in physical memory.

Fig. 6 shows the intrusion detection procedure toward illegal writing in physical memory. The procedure starts with checking out the event log whether the spying domain has been set. If not, illegal writing will be decided and an alerting signal is sent out. Otherwise, according to the addresses in the event log, the spying domain will be read to verify whether the hash result of secret information is correct. If the hash results are incorrect, illegal writing is decided and an alerting signal is sent out. If the hash results are correct, the event log will be further examined. If a legal reading command from utilities has been received and the network connection is unavailable, the writing is legitimate; otherwise, an alert will be sent.

2) Collaborative Intrusion Detection Procedure Toward Illegal Reading in Physical Memory: Collaborative intrusion detection of illegal reading is based on two important events in a smart meter.

1) Storage units in the physical memory will be cleared after being read, so illegal reading is likely to cause spying domain to be emptied.
2) Legitimate reading in physical memory occur when the disrupted network connection is available again and consumption data read from physical memory will be sent via network interface. Attackers usually disrupt network connections to write consumption data into the physical memory. Then, they read the physical memory illegally and transmit the consumption data via secret ways. In this case, no data are sent by the network interface.

Fig. 7 shows the intrusion detection procedure toward illegal writing in the physical memory. The procedure starts with accessing the event log to obtain addresses of the spying domain. Then, it examines if the spying domain has been cleared. If the result is true, a confirmation whether data has been sent normally via the network interface will be made. If no data have been sent, illegal reading is detected.

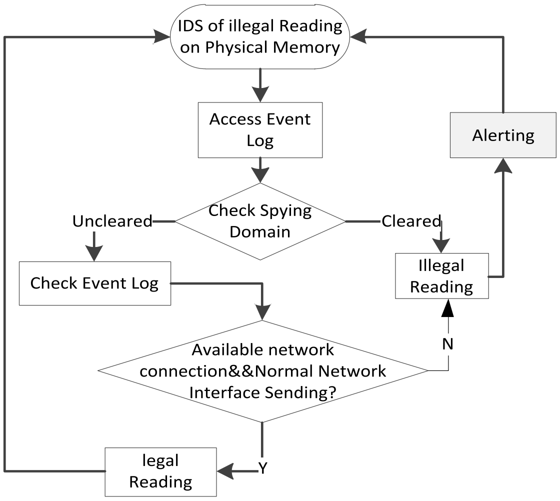
IDS of illegal Reading on Physical Memory
Access Event Log
Alerting
Check Spying Domain
Uncleared
Cleared
Check Event Log
Illegal Reading
N
Available network connection&&Normal Network Interface Sending?
Y
legal Reading

Fig. 7. Collaborative intrusion detection procedure toward illegal reading in physical memory.

When the attackers are powerful ones who may have analyzed a smart meter's software and stolen the secret information in advance. Then, they listen to the network interface to make sure that commands from utility companies are received by smart meters. The attackers disrupt the network connection to cause consumption data written into the physical memory.

Finally, with the stolen secret information, attackers can read or write the physical memory successfully without being detected. The powerful attackers may even tamper with the event log to clear their attack traces. However, to cope with those powerful attackers, we propose the following technique in the collaborative intrusion detection mechanism.

1) We encrypt communications to resist eavesdropping and thus prevent attackers from finding the best moment to launch an attack.
2) We update the secret information of a smart meter regularly to make the stolen ones useless.

In the design of the collaborative intrusion detection, we have defined the legitimate reading and writing operations and analyzed possible attack scenarios. Our intrusion detection mechanism can achieve signature-based detection by using secret information and anomaly-based detection by setting spying domain and defining legitimate reading and writing. Furthermore, signature-based IDS with a blacklist approach is suitable to identify known attacks while anomaly-based IDS with a whitelist approach is suitable to detect unknown attacks. As a consequence, our proposed collaborative intrusion detection mechanism can cope with both known and unknown attacks.

V. Performance Evaluation

The spying domain is the key concept in the collaborative intrusion detection mechanism. Its efficiency and cost determine the performance of the detection mechanism. In addition, due to the constrained computing and storage resources of a smart meter, it is very important to verify the spying domain's effectiveness and evaluate the cost of setting the spying domain. There are three key parameters to evaluate the spying domain. The intrusion detection rate is used to evaluate the effectiveness of spying domain. The higher the intrusion detection rate is, the more effective the spying domain is. Let M denote the cost of spying domain. M is the ratio between the total size of storage units used as the spying domain accounts for the size of the whole physical memory. Let N denote the strength of illegal reading or writing in the physical memory. N is the ratio between the size of the storage units read or written illegally and the size of the whole physical memory.

Smart meters are very limited by computing and storage resources. We propose several evaluation criteria when the spying domain should reach an relatively high intrusion detection rate with relatively low computation and storage cost. The evaluation criteria proposed in this paper are as follows.

Criterion 1: M must be no more than $1/100$, which is the basic evaluation criterion.

Criterion 2: When $N \geq 1/10$, the intrusion detection rate must achieve 100%.

Criterion 3: When $1/10 > N \geq 1/20$, the intrusion detection rate must be over 95%.

Criterion 4: When $1/20 > N \geq 1/50$, the intrusion detection rate must be over 75%.

It is noteworthy that the intrusion detection rates 100%, 95%, and 75% are based on the experimental results from [16]. Experiments have shown that the model-based IDS provides an average intrusion detection rate 69.6%. The intrusion detection rates set for the evaluation criteria of the spying domain are much higher than 69.6% because the performance of the collaborative intrusion detection mechanism is also influenced by operations on the event log as well as the secret information and failures may occur sometimes.

A. Simulation Design

The simulation has been performed through designing a program which can achieve the following functions.

1) Using an array with 10 000 B to represent physical memory of a smart meter.
2) Discontinuous storage units are chosen randomly from the array to represent the spying domain.
3) A subprogram imitates the malicious codes to perform illegal writing or reading on the "physical memory."
4) At last, the "spying domain" is checked out whether it has been operated. If the result is yes, a successful detection will be recorded.

Considering the evaluation criteria and aiming to get more reliable experimental results, the simulation experiments are performed under the following distinct conditions.

1) First Set of Conditions: Different sizes of spying domain including 100 B($M = 1/100$), 95 B($M = 0.95/100$), 90 B($M = 0.90/100$), 85 B($M = 0.85/100$), 80 B($M = 0.80/100$), 75 B($M = 0.75/100$), 70 B($M = 0.70/100$), 65 B($M = 0.65/100$), and 60 B($M = 0.60/100$) when the size of data read or written illegally keeps unchanged at 1000 B($N = 1/10$), 500 B($N = 1/20$), and 200 B($N = 1/50$), respectively.

2) Second Set of Conditions: Different sizes of data read or written illegally in the physical memory including 1300 B($N = 1.3/10$), 1200 B($N = 1.2/10$), 1100 B($N = 1.1/10$), 1000 B($N = 1/10$), 900 B($N = 0.9/10$), 800 B($N = 0.8/10$),

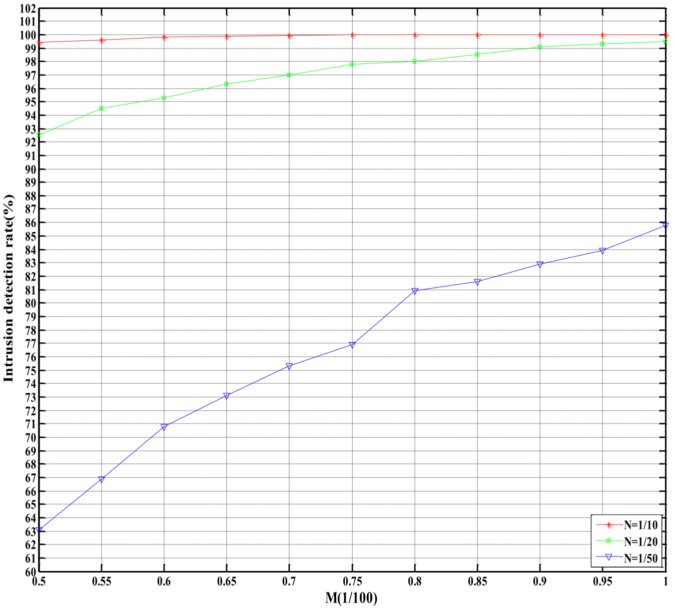

Fig. 8. Intrusion detection rate in terms of ***M*** with different ***N***.

700 B($N = 0.7/10$), 600 B($N = 1.2/20$), 500 B($N = 1/20$), 400 B($N = 0.8/20$), 300 B($N = 1.5/50$), and 200 B($N = 1/50$) when the size of spying domain keeps unchanged.

Under each condition, the simulation program run 1000 times such that we can have an accurate intrusion detection rate of the spying domain.

B. Simulation Results

Fig. 8 shows the intrusion detection rate in terms of M under the first set of conditions. The results indicate that the intrusion detection rate increases with higher M. In particular, when $M \geq 0.75/100$, the intrusion detection rates of $N = 1/10$ achieve 100%; the intrusion detection rates of $N = 1/20$ get over 97%; and the intrusion detection rates exceed 75% when $N = 1/50$. That is to say, when $M \geq 0.75/100$ the results meet all the evaluation criteria in this paper. Hence, to some extent, the spying domain of the collaborative intrusion detection is effective and low cost. Fig. 7 also suggests M to be set 0.75/100 for the spying domain since 0.75/100 is the smallest value for M to meet the evaluation criteria.

Fig. 9 shows the intrusion detection rates in terms of $\boldsymbol{N}$ with different M under the second set of conditions. When $N \geq 1/10$, the intrusion detection rates of $M = 0.70/100$ or $M = 0.75/100$ do not all reach 100%. For example, when $N = 1.1/10$, the intrusion detection rates of $M = 0.70/100$ and $M = 0.75/100$ are 99.96% and 99.99%, respectively. In contrast, when $M = 0.80/100$, the intrusion detection rates of $N \geq 1/10$ achieve 100%, which meet the evaluation criterion 2. Furthermore, the intrusion detection rates of the spying domain when $M = 0.80/100$ meet all the evaluation criteria.

Comparing Figs. 8 and 9, we can conclude that the following.

1) The spying domain is effective and low cost according the three evaluation criteria proposed.
2) It is appropriate to set $\boldsymbol{M}$ with the value 0.80/100 for spying domain because it is the smallest value among those satisfying all the evaluation criteria. That is to say, assume that the total size of physical memory is 20000 B, 160 B storage units should be chosen as the spying domain, which can achieve relatively high intrusion detection rate with relatively low cost.

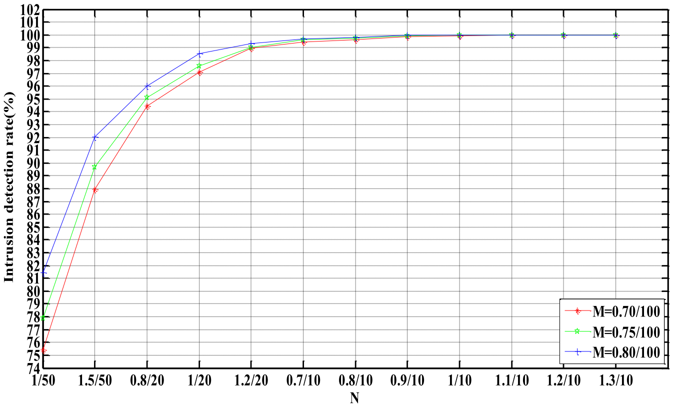

Fig. 9. Intrusion detection rate in terms of ***N*** with different ***M***.

VI. Conclusion

Smart meters security is a critical part of the smart grid and AMI networks. In this paper, we exploited the colored Petri net to describe the data and the commands flows in a smart meter, based on which threat model is built. We then proposed a collaborative intrusion detection mechanism composed of spying domain, event log and secret information for smart meters. This intrusion detection mechanism focuses on the false data injection attack and can work regardless of changes in software. Illustrative results have shown the effectiveness and low cost of the proposed scheme and suggested the key parameter determination. An interesting future topic is the reliable and effective updating mechanisms for smart meters' secret information.

References

[1] J. Zhong, R. Zheng, and W. Yang, "Construction of smart grid at information age," *Power Syst. Technol.*, vol. 33, no. 13, pp. 12–18, 2009.

[2] Y. Yu, "Technical composition of smart grid and its implementation sequence," *South. Power Syst. Technol.*, vol. 3, no. 2, pp. 1–5, 2009.

[3] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, 2011.

[4] R. David and H. Alla, *Discrete, Continuous, and Hybrid Petri Nets*. Berlin, Germany: Springer-Verlag, 2005, pp. 289–294.

[5] K. Jensen and L. Kristensen, *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*. Berlin, Germany: Springer-Verlag, 2009, pp. 193–198.

[6] J. McDermott, "Attack net penetration testing," in *Proc. Workshop New Security Paradigms (NSPW),* Cork, Ireland, 2000, pp. 15–21.

[7] G. Dalton, R. Mills, J. Colombi, and R. Raines, "Analyzing attack trees using generalized stochastic Petri nets," in *Proc. IEEE Workshop Inf. Assur.,* West Point, NY, USA, 2006, pp. 116–123.

[8] R. Wu, W. Li, and H. Huang, "An attack modeling based on hierarchical colored Petri nets," in *Proc. IEEE Int. Conf. Comput. Elect. Eng. (ICCEE),* Phuket, Thailand, 2008, pp. 918–921.

[9] K. Schneider, C.-C. Liu, and J.-P. Paul, "Assessment of interactions between power and telecommunications infrastructures," *IEEE Trans. Power Syst.*, vol. 21, no. 3, pp. 1123–1130, Aug. 2006.

[10] O. Gursesli and A. Desrochers, "Modeling infrastructure interdependencies using Petri nets," in *Proc. IEEE Int. Conf. Syst.*, vol. 2. Washington, DC, USA, 2003, pp. 1506–1512.

[11] J.-C. Laprie, K. Kanoun, and M. Kaaniche, “Modelling interdependencies between the electricity and information infrastructures,” in *Proc. 26th Int. Conf. Comput. Safety Rel. Security (SAFECOMP),* Nuremberg, Germany, 2007, pp. 54–67.

[12] V. Calderaro, C. N. Hadjicostis, A. Piccolo, and P. Siano, “Failure identification in smart grids based on petri net modeling,” *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4613–4623, Sep. 2011.

[13] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, “Petri net modeling of cyber-physical attacks on smart grid,” *IEEE Trans. Smart Grid,* vol. 2, no. 4, pp. 741–749, Apr. 2011.

[14] R. Berthier and W. H. Sanders, “Specification-based intrusion detection for advanced metering infrastructures,” in *Proc. Pac. Rim Int. Symp. Depend. Comput. (PRDC),* Pasadena, CA, USA, 2011, pp. 184–193.

[15] M. LeMay, G. Gross, C. A. Gunter, and S. Garg, “Unified architecture for large-scale attested metering,” in *Proc. 40th Annu. Hawii Int. Conf. Syst. Sci. (HICCS),* Waikoloa, HI, USA, 2007, pp. 126–135.

[16] F. M. Tabrizi and K. Pattabiraman, “A model-based intrusion detection system for smart meters,” in *Proc. IEEE 15th Int. Symp. High-Assur. Syst. Eng. (HASE)*, Miami Beach, FL, USA, 2014, pp. 17–24.

[17] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, “Securing advanced metering infrastructure using intrusion detection system with data stream mining,” in *Proc. Pac. Asia Workshop Intell. Security Informat.,* Kuala Lumpur, Malaysia, 2012, pp. 96–111.

[18] Y. Chongyi, *Principles and Applications of Petri Net*, Beijing, China: Electron. Ind. Press, 2005, p. 16.

[19] J. Peterson, “Petri nets,” *ACM Comput. Surv.*, vol. 9, pp. 223–252, Sep. 1977.

[20] M. Diaz, *Petri Nets: Fundamental Models, Verification and Applications.* Hoboken, NJ, USA: Wiley, 2009.

[21] V. Kordic, *Petri Net Theory and Applications*. Vienna, Austria: I-Tech Educ., 2008.

[22] K. Jensen, “Coloured Petri nets,” in *Proc. IEE Colloq. Discrete Event Syst. New Challenge Intell. Control Syst.*, London, U.K., May 1993, pp. 5.1–5.3.

[23] F. M. Cleveland, “Cyber security issues for advanced metering infrastructure (AMI),” in *Proc. IEEE Power Energy Soc. Gen. Meeting Convers.*, Pittsburgh, PA, USA, 2008, pp. 1–5.

[24] H. Khurana, M. Hadley, L. Ning, and D. Frincke, “Smart-grid security issues,” *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.

[25] T. Chen, “Survey of cyber security issues in smart grids,” *Proc. SPIE Cyber Security Situation Manage. Impact Assess. II Vis. Anal. Homeland Defense Security II*, vol. 7709, Apr. 2010, Art. ID 77090D.

[26] AMI System Security Requirements v1.01. (Dec. 2008). *AMI Security Acceleration Project AMI-SEC Task Force (AMI-SEC-ASAP).* [Online]. Available: http://www.oe.energy.gov/Documentsand-Media/14AMI_System_Security_Requirements.pdf

[27] Security Profile for Advanced Metering Infrastructure. (Dec. 2009). *Advanced Security Acceleration Project (ASAP-SG).* Knoxville, TN, USA. [Online]. Available: http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAPSG)/AMI%20Security%20Profile%20-%20v1_0.pdf

[28] W. Sikora, M. Carpenter, and J. Wright, *Smart Grid and AMI Security Concerns*, InGuardians Ind. Defend., Washington, DC, USA, 2009, pp. 88–90. [Online]. Available: http://inguardians.com/pubs/Smart_Grid_AMI_Security_Concerns-20090723.pdf

[29] J. Wright (InGuardians), (2010). *Smart Meters Have Security Holes*. [Online]. Available: http://www.msnbc.msn.com/id/36055667

[30] M. Davis, “Smart grid device security,” presented at BlackHat, Las Vegas, NV, USA, 2009. [Online]. Available: http://www.blackhat.com/presentations/com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf

[31] A. Metke and R. Ekl, “Smart grid security technology,” in *Proc. Innov. Smart Grid Technol*, Gaithersburg, MD, USA, 2010, pp. 1–7.

[32] A. Hamlyn *et al.*, “Computer network security management and authentication of smart grids operations,” in *Proc. IEEE Power Energy Soc. Gen. Meeting Convers.*, Pittsburgh, PA, USA, 2008, pp. 1–7.

[33] S. McLaughlin, D. Podkuiko, and P. McDaniel, “Energy theft in the advanced metering infrastructure,” in *Proc. 4th Int. Workshop Crit. Inf. Infrastruct. Security,* Bonn, Germany, Sep. 2009, pp. 176–187.

[34] T. A. Hawk. (Aug. 2014). *Smart Grid Security*. [Online]. Available: http://wnss.sv.cmu.edu/courses/14814/s12/files/adHawks_14814s12_22.pdf

[35] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2012, p. 340.

[36] R. Berthier, W. H. Sanders, and H. Khurana, “Intrusion detection for advanced metering infrastructures: Requirements and architecture directions,” in *Proc. IEEE Smart Grid Commun.*, Gaithersburg, MD, USA, 2010, pp. 350–355.

[37] D. Grochocki *et al.*, “AMI threats, intrusion detection requirements and deployment recommendations,” in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun.*, Tainan, Taiwan, 2012, pp. 395–400.

[38] S. McLaughlin, B. Holbert, S. Zonouz, and R. Berthier, “AMIDS: A multi-sensor energy theft detection framework for advanced metering infrastructures,” in *Proc. IEEE Smart Grid Commun. (SmartGridComm)*, Tainan, Taiwan, 2012, pp. 350–355.

[39] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention systems (IDPS),” U.S. Dept. Commer., Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Tech. Rep. 800-94, 2007. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[40] H. Debar, M. Dacier, and A. Wespi, “A revised taxonomy for intrusion-detection systems,” *Ann. Telecommun.*, vol. 55, no. 7, pp. 361–378, 2000.

[41] T. H. Ptacek and T. N. Newsham, “Insertion, evasion, and denial of service: Eluding network intrusion detection,” DTIC Document DTIC-IA, Secure Netw. Inc., Syracuse, NY, USA, 1998.

[42] C. Cowan *et al.*, “StackGuard: Automatic adaptive detection and prevention of buffer-overflow attacks,” in *Proc. 7th Conf. USENIX Security Symp*. vol. 7. Berkeley, CA, USA, 1998, pp. 63–78.

[43] G. Richarte, (2002). *Four Different Tricks to Bypass StackShield and StackGuard Protection.* [Online]. Available: http://www1.corest.com/files/files/11/StackGuardPaper.pdf

[44] S. J. Templeton and K. Levitt, “A requires/provides model for computer attacks,” in *Proc. Workshop New Security Paradigms*, Cork, Ireland, 2000, pp. 31–38.

Xiaoxue Liu (S’15) received the B.S. degree in information security from the Nanjing University of Aeronautics and Astronautics, Jiangsu, China, and the M.S. degree in computer science and technology from the National University of Defense Technology, Changsha, China, in 2012 and 2014, respectively, where she is currently pursuing the Ph.D. degree from the School of Computer.

Her current research interests include security of cyber-physical systems and Smart Grid security.

Peidong Zhu (SM’11) received the Ph.D. degree in computer science from the National University of Defense Technology (NUDT), Changsha, China, in 1999.

He is a Professor with the School of Computer Science, NUDT. His current research interests include network routing, network security, and architecture design of the Internet and various wireless networks. In 2008, he was the Visiting Professor with St. Francis Xavier University, Antigonish, NS, Canada, for one year.

Yan Zhang (M’05–SM’10) received the Ph.D. degree in electrical and electronics engineering from Nanyang Technological University, Singapore, in 2005.

He is currently with the Simula Research Laboratory, Lysaker, Norway. He is an Adjunct Associate Professor with the University of Oslo, Oslo, Norway. His current research interests include cognitive radio, smart grid, and machine-to-machine communications.

Dr. Zhang is an Associate Editor and a Guest Editor for a number of international journals. He serves as an Organizing Committee Chair for several international conferences.

Kan Chen received the B.S. and M.S. degrees from the National University of Defense Technology, Changsha, China, in 2007 and 2010, respectively, both in computer network engineering, where he is currently pursuing the Ph.D. degree with the School of Computer Science.

His current research interests include social network and network security.