IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INTERNET-OF-THINGS (IOT) BIG DATA TRUST MANAGEMENT

Received October 1, 2017, accepted October 28, 2017, date of publication November 13, 2017, date of current version March 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2772294

Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data

WEIZHI MENG[1], (Member, IEEE), WENJUAN LI[1,2], (Student Member, IEEE), CHUNHUA SU[3], JIANYING ZHOU[4], AND RONGXING LU[5], (Senior Member, IEEE)

[1]Department of Applied Mathematics and Computer Science, Technical University of Denmark, 2800 Lyngby, Denmark
[2]Department of Computer Science, City University of Hong Kong, Hong Kong
[3]Division of Computer Science, University of Aizu, Aizuwakamatsu 965-8580, Japan
[4]Information Systems Technology and Design, Singapore University of Technology and Design, Singapore 487372
[5]Faculty of Computer Science, University of New Brunswick, Saint John, E3B 5A3NB, Canada

Corresponding author: Chunhua Su (chsu@u-aizu.ac.jp)

This work was supported in part by JSPS Grants-in-Aid for Scientific Research KAKENHI under Grant WAKATE B-15K16005, in part by the Competitive Research Funding from the University of Aizu P-21, and in part by SUTD start-up Research Grant SRG-ISTD-2017-124.

ABSTRACT Internet of Things (IoT) has been widely used in our daily life, which enables various objects to be interconnected for data exchange, including physical devices, vehicles, and other items embedded with network connectivity. Wireless sensor network (WSN) is a vital application of IoT, providing many kinds of information among sensors, whereas such network is vulnerable to a wide range of attacks, especially insider attacks, due to its natural environment and inherent unreliable transmission. To safeguard its security, intrusion detection systems (IDSs) are widely adopted in a WSN to defend against insider attacks through implementing proper trust-based mechanisms. However, in the era of big data, sensors may generate excessive information and data, which could degrade the effectiveness of trust computation. In this paper, we focus on this challenge and propose a way of combining Bayesian-based trust management with traffic sampling for wireless intrusion detection under a hierarchical structure. In the evaluation, we investigate the performance of our approach in both a simulated and a real network environment. Experimental results demonstrate that packet-based trust management would become ineffective in a heavy traffic environment, and that our approach can help lighten the burden of IDSs in handling traffic, while maintaining the detection of insider attacks.

INDEX TERMS Intrusion detection, traffic sampling, wireless sensor network, trust computation, Bayesian model, big data.

I. INTRODUCTION

The Internet of Things (IoT) can be considered as the network of physical devices, vehicles, and other items embedded with various sensors and Internet connection [27], [40]. IoT allows interconnected objects to be sensed and controlled remotely under certain network framework, leading to a direct combination of physical world and computational systems. The interconnection of these objects are expected to provide unique identifiers and the ability to transfer data over a network with reduced human intervention [3], [35]. Nowadays, IoT has been popularly applied into our daily life, including smart home, wearables, building management, healthcare, energy and transportation.

Wireless sensor networks (WSNs) are an important part of IoT applications, which usually consist of various small, resource-limited, and autonomous sensor nodes (SNs) to transmit data and provide access points for humans. WSNs have been widely used in many fields such as agriculture [7], transportation [10] and homeland security [18]. Due to its inherent features like being deployed in a hostile environment and unreliability of transmission, this kind of network is vulnerable to a wide range of threats [8]. For example, cyber-criminals may try to exploit rogue or poorly configured access points of an organization to launch man-in-the-middle attacks, or steal users' data by placing an unauthorized hotspot to cheat users [21]. As a result, there is a need to

deploy appropriate security mechanisms to protect WSNs in practice.

To safeguard the security of WSNs, intrusion detection systems (IDSs) are one of the widely adopted and deployed security mechanisms [1], [21], [41]. Generally, an IDS can be categorized into signature-based IDS and anomaly-based IDS. The former (or called misuse detection) identifies potential attacks by comparing current observed events with its stored signatures [37]. A *signature* is a type of descriptions for a known attack or exploit. By contrast, the latter can detect anomalies by identifying significant deviations between the pre-established normal profile and the current events. In both cases, an alarm would be generated if any signature is matched, or the deviation above a threshold.

In real-world scenarios, WSNs are found to suffer from many types of attacks, especially insider attacks in which a malicious attack is performed on a computer network by an intruder with authorized system access [5]. To identify a malicious node, IDSs usually employ trust management approaches to evaluate the trustworthiness of WSN nodes. A hierarchical structure is commonly used aiming to reduce network traffic caused by node-to-node communications. Examining the packet status is a promising way to detect insider attacks [29]. However, in the era of big data, how to perform trust computation is a challenge, since sensor nodes may generate a large amount of data like packets.

In a conventional network, massive network packets are already a big issue for an IDS, in which the traffic may greatly exceed the maximum processing capability of an IDS [36]. With the rapid development of Internet, data volumes during the communication have become significantly large and might result in many security issues. For example, it is very likely for an IDS to drop many packets in a heavy traffic environment. This situation in the era of big data would become even more complex than that in a typical network [33]. In this case, trust computation based on traditional packets' status becomes difficult; thus, there is a need to make a better tradeoff to identify insider attacks in the big data era.

Contributions: Motivated by this challenge, in this paper, we conduct an early study by proposing a trust management approach using traffic sampling for wireless intrusion detection. In particular, we focus on the Bayesian-based trust computation, which was given in our previous work [29], and investigate its performance in heavy traffic environments. This kind of trust-based intrusion detection mechanisms can evaluate the trustworthiness of a sensor node based on its packet status sent in a hierarchical WSN, and detect malicious nodes by selecting an appropriate trust threshold. The contributions of this work can be summarized as below.

- We focus on a scalable and hierarchical structure of WSNs, including sensor nodes (SNs) and cluster heads (CHs), where a node can record packets' status during the node-to-node communication, and a CH is responsible for collecting and calculating trust values for all nodes. Based on this structure, we propose a way of combining Bayesian-based trust management approach with traffic sampling to evaluate the trustworthiness of a node in a heavy traffic environment.
- In the evaluation, we conduct two major experiments in both a simulated and a real network environment to investigate the performance of our approach against insider attacks, e.g., betrayal attacks. Experimental results demonstrate that by selecting an appropriate trust threshold, our approach can enhance the trust management in a high-traffic scenario, and is effective in detecting malicious nodes while reducing the burden of an IDS in handling traffic. Our work aims to complement the existing results and stimulate more research in this area.

The reminder of this paper is organized as follows. In Section II, we review relevant studies about trust computation and management in a WSN. Section III introduces the Bayesian-based trust management and describes two methods of traffic sampling. In Section IV, we evaluate the performance of our approach in both a simulated and a real network environment under heavy traffic scenarios. We make a discussion in Section V and conclude our work in Section VI.

II. RELATED WORK AND BACKGROUND

Trust management in computer science aims to evaluate and predict the behavior of target objects [16]. Distributed systems and networks like WSNs often employ trust-based security mechanisms to help identify abnormal events and nodes [11].

Probst and Kasera [38] described how to establish trust management among sensor nodes to detect malicious sensor nodes and minimize their influence on applications. They proposed a method to compute statistical trust values and a confidence interval around the trust, according to the behaviors of sensor nodes. Wang *et al.* [39] presented *IDMTM*, a trust-based intrusion detection mechanism for mobile ad hoc networks. Their approach evaluated the trust and identify a malicious node by using two developed metrics: Evidence Chain (EC) and Trust Fluctuation (TF), which could greatly decrease the false alarm rate by efficiently utilizing the information collected from both the local nodes and the neighboring nodes. Chen *et al.* [9] focused on WSNs and proposed an event-based trust framework, which utilized a watchdog scheme to monitor the behavior of nodes and broadcast their trust ratings. They defined many levels of trust-rating values for different sensor events. More specifically, a sensor node could have more than one trust-rating value stored in its neighbor nodes. Then, Zahariadis *et al.* [48] proposed a routing protocol (ATSR) based on geographical routing principle, which could cope with the network dimensions. This makes ATSR be able to detect malicious neighbors by means of a distributed trust model considering both direct and indirect trust information.

For group trust management, Shaikh *et al.* [42] developed a lightweight Group-based Trust Management Scheme (GTMS) for wireless sensor networks. The scheme evaluated the group trust of sensor nodes and worked

in two situations: the first situation is *intragroup topology* where a distributed trust management approach was designed, and the other is *intergroup topology* where a centralized trust management approach was employed. Similarly, Zhang *et al.* [49] proposed a dynamic trust establishment and management framework for hierarchical wireless sensor networks. Their consider both direct and indirect (group) trust for reputation computation as well as the energy associated with sensor nodes in service selection. They further considered the dynamic nature of trust and proposed a trust varying function, which could give more weight to the most recently obtained trust values in the trust computation. The hierarchical structure including base station, clusters and sensor nodes adopted in this work is very similar to their work, which is believed to help reduce traffic among different nodes.

Guo *et al.* [19] proposed a trust management framework based on Grey theory and Fuzzy sets, where the total trust was computed by considering relation factors and weights of neighbor nodes. Bao *et al.* [5] developed a trust-based intrusion detection scheme for a hierarchical wireless sensor networks by considering both quality of service (QoS) trust and social trust for detecting malicious nodes. They built an analytical model based on stochastic Petri nets for performance evaluation and detailed a statistical method for calculating the probability of false alarm generation. The results showed that there existed an optimal trust threshold for minimizing false positives and false negatives, which could vary with the anticipated WSN lifetime. They further validated their algorithm with traditional anomaly-based detection techniques such as weighted summation-based IDS and fixed width data clustering-based IDS, and found that their proposed scheme could achieve better detection performance with lower false positives (i.e., less than 5%) [6]. Several other related work regarding trust-based intrusion detection mechanisms can be referred to [13], [15], [22]–[25], [31], [32], [44].

In the previous work [29], we investigated how to evaluate the trustworthiness of WSN nodes by examining the packets' status via Bayesian model and studied the impact of both a fixed and a dynamic trust threshold on identifying malicious nodes. However, in the era of big data, it is very difficult for an IDS to handle massive incoming packets, resulting in an ineffective process of trust computation. Motivated by this issue, our work presents an initial study to explore how to perform trust computation in a heavy traffic environment via traffic sampling.

III. OUR APPROACH

In this section, we present the typical architecture of hierarchical (clustered) wireless sensor networks, describe the Bayesian-based intrusion detection mechanism and how to compute the trustworthiness of a sensor node by means of Bayesian model, and detail the adopted traffic sampling approaches.

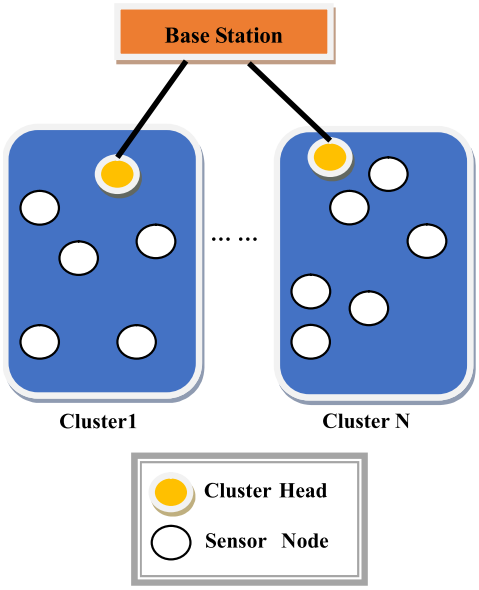

FIGURE 1. The typical architecture of hierarchical wireless sensor network.

A. HIERARCHICAL WIRELESS SENSOR NETWORK

A WSN with hierarchical structure is usually composed of a base station, multiple clusters and sensor nodes. Generally, each cluster contains a cluster head (CH) and a set of sensor nodes (SNs), where a cluster head is assumed to have more computational power and energy resources than a node. Fig. 1 depicts a typical high-level architecture of a hierarchical WSN. It mainly consists of a base station, several cluster heads and many clusters (e.g., Cluster 1, Cluster 2,..., Cluster N) that can be grouped by multiple sensor nodes.

It is worth noting that a cluster head in each cluster can be selected through various election protocols (e.g., [47]), and a cluster can be grouped according to different criteria [49] like location and communication range or using specific cluster algorithms [20]. In particular, a sensor node transmits the data to its corresponding cluster head, and then the cluster head transmits the data to the base station. There are some basic assumptions for a hierarchical WSN as follows:

- All sensor nodes and cluster heads are stationary. That is, the physical locations and the communication range of all nodes are known.
- Each sensor node and cluster head have their unique identities and all nodes are organized into clusters.
- The base station is a central control authority and virtually has no resource constraints, which is fully trusted by all nodes.
- Cluster heads have more computational power and memory as compared with those sensor nodes within a WSN.
- The base station communicates data with the cluster head directly, while each cluster head is responsible for managing all sensor nodes in the cluster.

To protect WSNs against attacks, an IDS is usually deployed in each node for collecting necessary data and

then the cluster head can compute the trust values of other nodes. In this work, we focus on the Bayesian-based trust management and adopt a signature-based IDS for each node. As each node has the capability of recording and transmitting packet, they can be considered as a *wireless signature-based detection sensor*.

B. BAYESIAN-BASED INTRUSION DETECTION MECHANISM

1) BAYESIAN MODEL

This is an inference approach (or called *Bayesian inference*) that uses Bayes' rule to update the probability estimate for a hypothesis as additional evidence [45]. In intrusion detection, this model can be applied for calculating the trust values for an object. In terms of traffic information, this model can be used to evaluate the trust worthiness of sensor nodes in a clustered WSN.

The main assumption is that all packets sent from a node are independent from each other. In other words, if one packet is found to be malicious, the probability of the following packet being a malicious packet is still equal. Actually, this assumption indicates that the attacks can appear in various forms, either in one packet or in a number of packets. To derive the computation of trust values, we assume that N packets are sent from a node, of which k packets are proven to be *normal*. Based on the results from previous work [16], [45], the distribution of observing $n(N) = k$ is governed by a Binomial distribution as below. [1]

$$P(n(N) = k|p) = \binom{N}{k} p^k (1-p)^{N-k} \tag{1}$$

where $P(n_i : normal) = p$ means the probability of the i^{th} packet is normal, V_i means that the i^{th} packet is normal, and $n(N)$ means the number of normal packets.

The real objective of Bayesian model is to estimate the probability of $P(V_{N+1} = 1|n(N) = k)$, determining whether the $N + 1$ packet is normal. Based on the Bayesian theorem, we can have the following probability distribution.

$$P(V_{N+1} = 1|n(N) = k) = \frac{P(V_{N+1} = 1, n(N) = k)}{P(n(N) = k)} \tag{2}$$

Then, we can apply marginal probability distribution, which is the probability distribution of the variables contained in the subset of random variables. We can have two equations as follows:

$$P(n(N) = k) = \int_0^1 P(n(N) = k|p) f(p) \cdot dp \tag{3}$$

$$P(V_{N+1} = 1, n(N) = k) = \int_0^1 P(n(N) = k|p) f(p) p \cdot dp \tag{4}$$

As there is no prior information about p, we assume that p is determined by a uniform prior distribution $f(p) = 1$ where $p \in [0, 1]$. To summarize Equation (1)-(4), we can have the following equation:

$$P(V_{N+1} = 1|n(N) = k) = \frac{\int_0^1 P(n(N) = k|p) f(p) p \cdot dp}{\int_0^1 P(n(N) = k|p) f(p) \cdot dp} = \frac{k+1}{N+2} \tag{5}$$

As a result, trust values (denoted t_{value}) can be calculated based on Equation (5) for all nodes in a WSN after collecting the traffic information, i.e., obtaining the number of normal packets k and the total number of packets N. By deciding an appropriate threshold, a malicious node can be identified accordingly. This model can help decide whether a node is malicious based on a set of traffic.

2) TRUST-BASED INTRUSION DETECTION MECHANISM

According to Equation (5), we have to record the total number of its sent packets and the number of normal packets. Taking a misuse-based IDS (e.g., Snort) as an example, the status of a packet can be determined by performing signature matching between incoming payloads and the stored IDS signatures. If we know the number of malicious packets is m, then we can compute the number of normal packets as: $k = N - m$. If we select a *trust threshold* of $T \in [a, b]$, then we can judge a malicious node as follows:

- If $t_{value} \geq T$, then the relevant node is considered to be a normal one.
- If $t_{value} < T$, then the relevant node is considered as a malicious (or untrusted) node.

3) TRUST COMPUTATION FOR A NODE

In a hierarchical WSN, each node could have two major functions: sensing and relaying. Sensor nodes collect data and then send the collected data to the corresponding cluster head directly in one hop or by relaying via a multi-hop path. Sensor nodes can transmit or relay data via short-haul radio communication. It is worth noting that each CH is able to control and reach all the sensor nodes within its cluster. In this case, a CH can receive the data from different sensor nodes, and then can process and compute trust values. In the end, CHs deliver the data to the base station. In this hierarchical structure, the trustworthiness of a CH should be evaluated by the base station.

Fig. 2 describes an example of data exchange in a hierarchical WSN. Each sensor node deployed with a signature-based IDS can record and transmit incoming packets. The trust computation is usually based on a time period of t, which consists of several time units. The sensor nodes in a cluster can record the traffic including the total number of outgoing packets and the number of malicious packets about other nodes in each time unit and then send the information to its cluster head. After several time units elapse, the time window slides to the right (e.g., one time unit), and the sensor nodes can drop the data collected during the earliest unit with the purpose of reducing storage consumption. After receiving the data, the

[1] Binomial distribution is the discrete probability distribution that represents the number of successes in a sequence of n independent, which the possibility of each n is the same p.

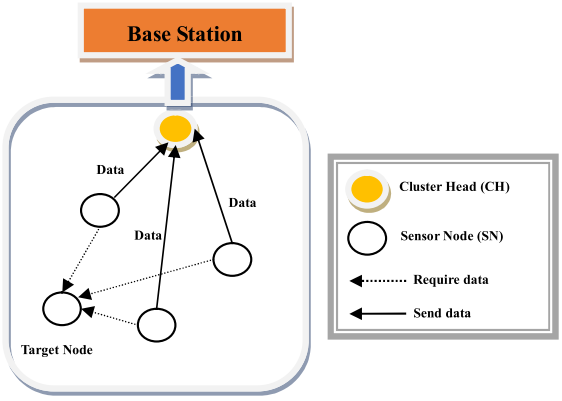

FIGURE 2. An example of data exchange in a hierarchical wireless sensor network.

cluster head can calculate the trust values for the target node during a selected time period based on Equation (5). In the end, the cluster head reports the results and sends data to the base station.

Further, the cluster head can periodically request the status of a target node and thus can establish a map of trust values. If a trust threshold is given, then the cluster head can quickly identify malicious nodes based on the matrix. In the mechanism, bad behavior of a node (i.e., sending malicious packets) can reduce its trust value greatly. For a sensor node, its trust value can be computed by its cluster head, while for a cluster head, its trust value can be computed by the base station.

C. TRUST MANAGEMENT VIA TRAFFIC SAMPLING

In the era of big data, traffic volumes could become extremely large, making a traditional IDS unable to handle such huge traffic (i.e., causing traffic overloaded and simply exceeding the processing capability). In a conventional network, overhead packets can greatly degrade the performance of IDSs as well as trust management. For example, the loss of packets can decrease the effectiveness of computing trust values relating to a target node in a WSN. Obviously, this issue would become even worse when meets big data scenarios.

To mitigate this issue, traffic sampling is a promising solution for anomaly detection. In this work, we advocate its effectiveness and apply this technique for trust management in a heavy traffic environment. Our goal is to investigate whether it can be used to reduce the burden of an IDS on inspecting traffic while maintaining the detection of insider attacks in a WSN. In literature, the use of sampling techniques aims to provision information about a specific characteristic of the parent population at a lower cost than a full examination. The sampling techniques can be generally classified into *packet-based* and *flow-based* samplings. The former mainly selects packets using either a deterministic or non-deterministic method, while the latter usually classifies packets into flows at first.

In literature, packet sampling has been well-studied in the aspect of network traffic measurements. For instance, Duffield *et al.* [14] proposed two inference methods for sampled flows, which could extract smoothed information about the flow length distribution. Xu *et al.* [46] targeted on how to keep and improve sampling accuracy during burst or fluctuation periods, and proposed an adaptive packet-level sampling method on different traffic fluctuation and burst scales. This method was able to dynamically adjust each packet sampling probability dependent on the magnitude of traffic fluctuation. Mai *et al.* [26] pointed out that sampling could post fundamental bias that degrades the effectiveness of portscan detection algorithms and dramatically increases false positives. Androulidakis and Papavassiliou [2] then analyzed flow-sampling techniques that have practical application in anomaly detection and proposed a flow-based sampling technique that focuses on the selection of small flows, which have a high probability to be the source of malicious traffic. Their results showed that even with small attack and sampling rates, the detection effectiveness is significantly improved while the number of packets required to be processed is reduced.

As an early study of combining trust management with traffic sampling, this work mainly focuses on packet sampling and investigate two statistical sampling techniques as below [2].

- **Systematic Sampling.** This technique starts the sampling process by selecting the start points and the duration of the selection intervals according to a deterministic function, where the triggers for starting sampling are periodic. All packets would be captured in a selection interval. To implement this approach, we can set the periodic selection of every $k - th$ packet.
- **Random n-out-of-N Sampling.** This sampling technique divides traffic population in bins of N packets each, and then n packets are randomly selected out of each bin. For instance, we can first randomly generate n different numbers in a range from 1 to N, and then select the packets that have a packet position equal to one of the numbers. For a stratified random sampling, we can set $n = 1$.

The selection of the above two sampling methods are due to their easy-understanding principles and widely adoption. They are the basic sampling methods in the area of packet sampling domain. It is worth noting that there are two basic kinds of statistical sampling categories: count-based sampling and time-based sampling. As time-based sampling may suffer from bias issues, i.e., missing burst periods with many packets [12], this work focuses on the count-based sampling, especially the above two sampling methods at this stage.

IV. EVALUATION

In this section, we mainly conduct two experiments to evaluate the performance of our proposed trust management via traffic sampling in a simulated and a real WSN environment, respectively.

- *Experiment-1*. This experiment aims to study the threshold in a simulated WSN with regular traffic. After deciding the normal threshold, we conducted a betrayal attack

by sending malicious packets through testing tools[2] (i.e., flooding the WSN with deauthentication packets-WVE-2005-0045).

- *Experiment-2*. In this experiment, we collaborated with an IT company to evaluate our approach in a practical WSN environment. This network consists of 13 cluster heads and more than 150 nodes. Similarly, during the attack period, malicious nodes can launch a betrayal attack by sending malicious packets.

A. EXPERIMENT-1

In this section, we conduct an experiment in a simulated environment. The simulated WSN consists of 100 sensor nodes (SNs) and 10 cluster heads (CHs) uniformly distributed in a 110m×110m area. The time unit for collecting traffic and computing trust values of nodes is set to 10 minutes. To investigate the trust values of nodes and the performance of our approach, we randomly selected five clusters and observed the results.

1) THRESHOLD

To efficiently identify malicious nodes via trust management, an important step is to select a proper trust threshold in advance. According to Equation (5), if k (the number of normal packets) increases its value, then t_{value} can become larger. Since k should be always smaller than N (the total number of incoming packets), t_{value} would fall into the interval of [0,1]. Thus, in the best scenario, t_{value} can be infinitely close to 1, indicating that a node is more credible by sending 'good' packets. By contrast, a decease of t_{value} means that malicious packets are detected for the corresponding sensor node. It is worth emphasizing that a node can be regarded as malicious by only sending one malicious packet, but this may case many false positives. Trust-based intrusion detection can provide more flexibility for reducing false rates and recovering a false detected node by adjusting the threshold.

If we denote a as the lower limit of trust threshold, then the threshold can be presented as $[a,1]$. In order to determine the lower limit a, we run the simulated network to observe the trend of trust values. The average trust values for five clusters are shown in Fig. 3.

The average trust values are computed by considering the trust values of all sensor nodes in a cluster within an hour. In this simulation, we consider an *hour* is an appropriate time unit for collecting and recording traffic, whereas the actual time duration can be easily configured in a real scenario, i.e., a security administrator can adjust it. The figure shows that the average trust values of each cluster are distinct. For example, the trust values of nodes in Cluster1, Cluster2 and Cluster5 ranged from 0.79 to 0.94, from 0.76 to 0.95, from 0.77 to 0.93, respectively.

If we look closer to the relationship between the time unit and the trust values, it is visible that the average values are

[2]http://code.google.com/p/wireless-intrusion-detection-system-testing-tool/.

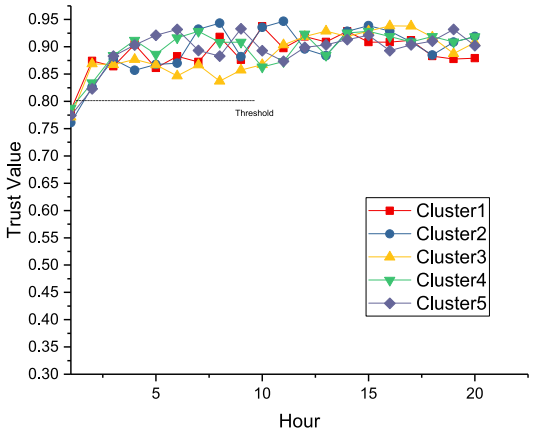

FIGURE 3. The average trust values for five randomly selected clusters in the simulated WSN.

mostly above 0.8 after the first hour. This is because the nodes in each cluster require some time to collect and exchange data until the whole network becomes stable. After the first time unit, the trust values of nodes in Cluster1, Cluster2 and Cluster5 ranged from 0.86 to 0.94, from 0.82 to 0.95, from 0.82 to 0.93, respectively. As a result, we select the threshold to 0.8 by considering the dynamic nature of traffic.

2) HEAVY TRAFFIC ADVERSARY SCENARIO

In this scenario, we consider that the wireless network is under both heavy traffic and a betrayal attack, where a benign node suddenly becomes malicious by launching attacks within the network. In this work, we consider two specific attack models: one is *maximal harm model* where the hostile nodes always send malicious packets; and the other is *random poisoning model*, where the hostile nodes send malicious packets in a random way [30]. For the heavy traffic, we simulated the network under a packet rate of 11,000 packets/sec. The average trust values of nodes for Cluster1 under the two attack models are depicted in Fig. 4 and Fig. 5, respectively.

- Under maximal harm model, Fig. 4 shows that in a regular traffic environment, the trust values of malicious nodes could decrease rapidly below the threshold of 0.8 after they launched an attack. In comparison, under heavy traffic environment, the trust values could still decrease but with a slow speed. It took seven hours for trust values to go below the threshold. This is because an IDS would discard packets when the incoming packets exceeded its handling capability. Regarding our approach of using traffic sampling, it is found that the trust values of malicious nodes under both systematic sampling and random sampling could decrease in a similar way as that in a regular traffic environment, i.e., these two sampling methods could decrease the trust values of malicious nodes below the threshold within an hour.
- Under random poisoning model, Fig. 5 demonstrates that in a regular traffic scenario, the trust values of

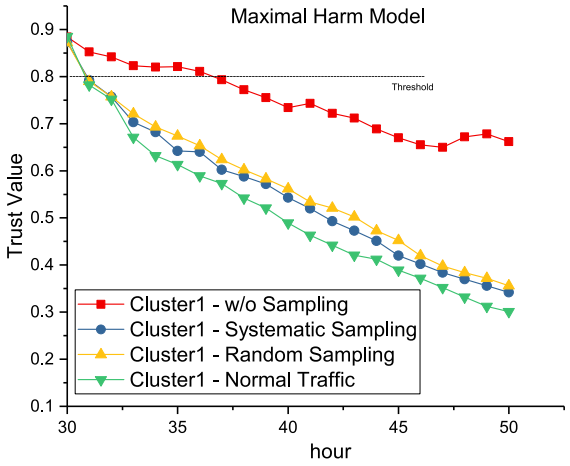

FIGURE 4. The average trust values of malicious nodes within Cluster1 in the simulated WSN, under heavy and hostile traffic (with maximal harm model).

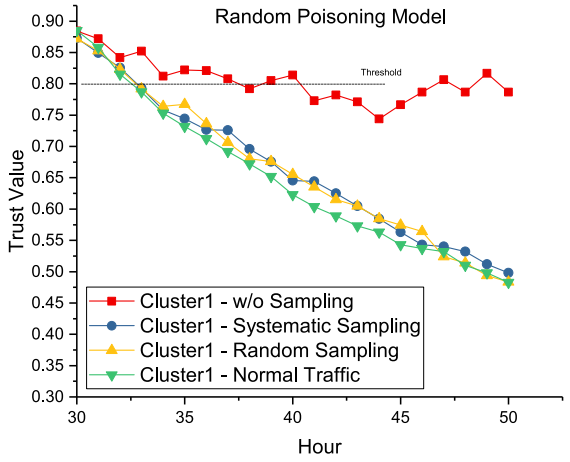

FIGURE 5. The average trust values of malicious nodes within Cluster1 in the simulated WSN, under heavy and hostile traffic (with random poisoning model).

malicious nodes require more time to go below the threshold as compared to the results under maximal harm model (i.e., two hours more). Under high traffic volumes, the trust values would decrease unsteadily, i.e., the value could go above the threshold again after a decrease. This is because an IDS would discard many packets due to limited handling capability, resulting in unstable detection of malicious packets. By contrast, our approach can achieve similar performance as that in a regular traffic environment, in which both sampling methods need two more hours to decrease the trust values of malicious nodes to below 0.8, as compared to the situation without sampling.

To summarize, trust management would become ineffective under heavy traffic volumes, due to that IDSs would discard a large number of packets. However, our approach with traffic sampling could reduce the number of packets needed to handle, while achieving similar performance as that in a regular traffic environment. That is, our approach

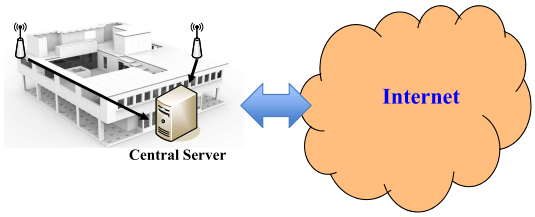

FIGURE 6. High-level architecture of the real WSN: a central server is deployed to collect data from sensor nodes.

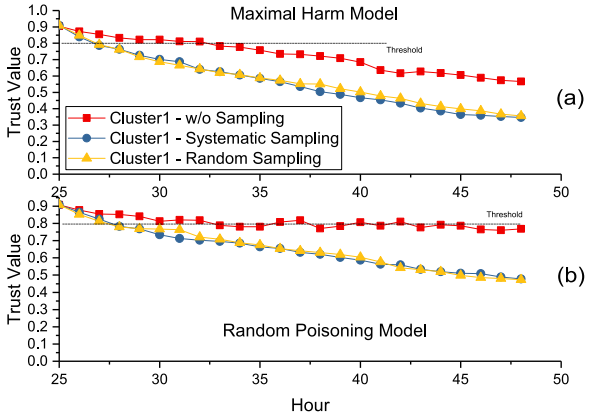

FIGURE 7. The average trust values of malicious nodes in the practical WSN under heavy traffic: (a) attacks based on maximal harm model, and (b) attacks based on random poisoning model.

can decrease the trust values of malicious nodes in a similar speed as that in a regular traffic scenario. The obtained results demonstrate that our approach can help enhance the trust management in a heavy traffic environment.

B. EXPERIMENT-2

In this experiment, we collaborated with a company to validate the performance of our approach in a real WSN environment. Fig. 6 shows a high-level architecture of the network environment. The WSN environment has a total of 13 clusters and more than 150 nodes. Due to privacy issues, we could only implement our approach in one cluster of this environment, whereas it is the biggest cluster with 58 nodes in this environment. This still provides a practical platform for our experiment. The incoming traffic on the cluster head is about 9,823 packets/s on average, while the maximum rate can reach 12,100 packets/s.

The basic settings are the same as the first experiment, and we set the threshold to 0.8. After deploying our approach, the trust values of sensor nodes in this network become stable after several hours. Then we randomly selected five sensor nodes to launch a betrayal attack by sending malicious packets under maximal harm model and random poisoning model, respectively. The average trust values of nodes under these two attack models are depicted in Fig. 7.

- Under maximal harm model, Fig. 7 (a) depicts that the trust values of malicious nodes could gradually decrease below the threshold of 0.8 under the heavy traffic

environment. As the attacks were launched under maximal harm model, malicious packets were easy to be captured and identified. However, due to the drop of packets especially malicious packets, the trust management was not effective in a heavy traffic environment. In comparison, our approach can enhance the trust computation in such condition, where the trust values of malicious nodes under both systematic sampling and random sampling could decrease faster (i.e., requiring only one hour versus seven hours without sampling).

- Under random poisoning model, Fig. 7 (b) shows a similar observation that the trust values of malicious nodes decreased unsteadily in the high-traffic volume environment. It is seen that the value was very close and even increased above the threshold several times. As a comparison, our approach could decrease the trust values of malicious nodes stably and faster, i.e., the two sampling methods required two hours to decrease the trust values of malicious nodes to below the threshold.

Overall, the experimental results validate that under a high-volume traffic scenario, packet-based trust management would become ineffective due to the loss of packets, i.e., it is hard to detect malicious nodes in a quick manner, making the whole system vulnerable to potential attacks. By contrast, our approach presents a faster speed of detecting malicious nodes in such situation, while lightening the burden of an IDS in handling overhead traffic.

V. DISCUSSION

This is an early study on investigating the application of traffic sampling to Bayesian-based trust management in the era of big data. The experiments have demonstrated some promising results; however, there are many issues that can be considered and improved in our future work.

- **Traffic sampling.** In this work, we only consider two statistical traffic sampling methods. There are many other sampling approaches can be explored in our future work, like flow-based sampling [2]. A flow can be regarded as a set of packets that have common features such as source IP address, source port, destination IP address, destination port and so on. In this case, sampling can be performed in flows by selecting all packets that belong to a particular flow.
- **Attack model.** Based on our experiments, it is observed that attack models can have an impact on the effectiveness of trust management. For example, it is easier to identify malicious nodes that launch attacks under maximal harm model than those under random poisoning model. In practice, cyber-criminals may conduct even more complicated attacks like PMFA [24]; thus, it is an interesting topic to investigate other attack models and identify the relationship between the sampling rate and detection rate.
- **Threshold selection.** Threshold is an important factor affecting the effectiveness of trust management. In real scenarios, threshold selection is usually depending on the features of a real network. In this work, we acknowledge that 0.8 is a suitable threshold for our settings and experimental environment. However, there is a need to explore and choose a specific threshold in other environments. This is an open challenge for trust management.
- **Heavy traffic and big data.** In this work, we investigate the performance of our approach in both a simulated and a real network environment under heavy traffic. The traffic rate was advised by our collaborated organization; however, it is always an interesting topic to validate our results in an environment with even heavier traffic. Security mechanisms need to be concerned with volume, variety and velocity in the big data era. One of our future work is thus to deploy and examine our approach in other places with high-volume traffic like a data center.

VI. CONCLUSION

Wireless sensor network (WSN) is an important application of IoT, which allows interconnected objects to be sensed and controlled, i.e., with a direct combination of physical world and computational systems. As such network is vulnerable to various attacks especially insider attacks, trust-based intrusion detection techniques are often adopted to protect its security. However, in the era of big data, packet-based trust management would become ineffective due to the overhead traffic and the dropping of packets. To mitigate this issue, in this work, we focus on Bayesian-based trust management and propose a way of combining it with traffic sampling for wireless intrusion detection. In the evaluation, we mainly conducted two experiments in both a simulated and a real network environment to investigate the performance of our approach against betrayal attacks. Experimental results demonstrate that a threshold of 0.8 is suitable for our experimental settings and that our approach can enhance the trust management in a high-traffic environment through detecting malicious nodes in a quick manner, while reducing the burden of an IDS in handling traffic. Our work attempts to stimulate more research on performing effective trust management for IoT in the era of big data.

REFERENCES

[1] A. Abduvaliyev, A. K. Pathan, J. Zhou, R. Roman, and L. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1223–1237, 3rd Quart., 2013.

[2] G. Androulidakis and S. Papavassiliou, "Improving network anomaly detection via selective flow-based sampling," *IET Commun.*, vol. 2, no. 3, pp. 399–409, Mar. 2008.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[4] S. Axelsson, "The base-rate fallacy and the difficulty of intrusion detection," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 3, pp. 186–205, Aug. 2000.

[5] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Trust-based intrusion detection in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2011, pp. 1–6.

[6] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Netw. Serv. Manage.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.

[7] R. Beckwith, D. Teibel, and P. Bowen, "Report from the field: Results from an agricultural wireless sensor network," in *Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw.*, Nov. 2004, pp. 471–478.

[8] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, 2nd Quart., 2009.

[9] H. Chen, H. Wu, J. Hu, and C. Gao, "Event-based trust framework model in wireless sensor networks," in *Proc. Int. Conf. Netw., Archit., Storage (NAS)*, Jun. 2008, pp. 359–364.

[10] S.-Y. Cheung and P. Varaiya. (2007). "Traffic surveillance by wireless sensor networks: Final report." Inst. Transp. Stud., Univ. California, Berkeley, Berkeley, CA, USA, California PATH Res. Rep. UCB-ITS-PRR-2007-4. [Online]. Available: http://www.its.berkeley.edu/publications/UCB/2007/PRR/UCB-ITS-PRR-2007-4.pdf

[11] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

[12] K. C. Claffy, G. C. Polyzos, and H.-W. Braun, "Application of sampling methodologies to network traffic characterization," in *Proc. ACM SIGCOMM*, San Francisco, CA, USA, 1993, pp. 13–17.

[13] K. Daabaj, M. Dixon, T. Koziniec, and K. Lee, "Trusted routing for resource-constrained wireless sensor networks," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Dec. 2010, pp. 666–671.

[14] N. Duffield, C. Lund, and M. Thorup, "Estimating flow distributions from sampled flow statistics," *IEEE/ACM Trans. Netw.*, vol. 13, no. 5, pp. 933–946, Oct. 2005.

[15] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 3, pp. 1–37, May 2008.

[16] J. M. Gonzalez, M. Anwar, and J. B. D. Joshi, "A trust-based approach against IP-spoofing attacks," in *Proc. 9th Int. Conf. Privacy, Secur. Trust (PST)*, Jul. 2011, pp. 63–70.

[17] A. K. Ghosh, J. Wanken, and F. Charron, "Detecting anomalous and unknown intrusions against programs," in *Proc. Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Dec. 1998, pp. 259–267.

[18] A. Grilo, K. Piotrowski, P. Langendoerfer, and A. Casaca, "A wireless sensor network architecture for homeland security application," in *Proc. 8th Int. Conf. Ad-Hoc, Mobile Wireless Netw. (ADHOC-NOW)*, 2009, pp. 397–402.

[19] J. Guo, A. Marshall, and B. Zhou, "A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks," in *Proc. 10th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Nov. 2011, pp. 142–149.

[20] G. Gupta and M. Younis, "Performance evaluation of load-balanced clustering of wireless sensor networks," in *Proc. 10th Int. Conf. Telecommun. (ICT)*, Feb./Mar. 2003, pp. 1577–1583.

[21] K. Hutchison, "Wireless intrusion detection systems," SANS, Melbourne, VIC, Australia, GSEC White Paper 1543, 2005, pp. 1–18. [Online]. Available: http://www.sans.org/reading_room/whitepapers/wireless/wireless-intrusion-detection-systems_1543

[22] W. Li, Y. Meng, and L.-F. Kwok, "Enhancing trust evaluation using intrusion sensitivity in collaborative intrusion detection networks: Feasibility and challenges," in *Proc. 9th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2013, pp. 518–522.

[23] W. Li, Y. Meng, and L.-F. Kwok, "Design of intrusion sensitivity-based trust management model for collaborative intrusion detection networks," in *Proc. 8th IFIP Int. Conf. Trust Manage. (IFIPTM)*, 2014, pp. 61–76.

[24] W. Li, W. Meng, L. F. Kwok, and H. H. S. Ip, "PMFA: Toward passive message fingerprint attacks on challenge-based collaborative intrusion detection networks," in *Proc. 10th Int. Conf. Netw. Syst. Secur. (NSS)*, 2016, pp. 433–449.

[25] K. Liu, N. Abu-Ghazaleh, and K.-D. Kang, "Location verification and trust management for resilient geographic routing," *J. Parallel Distrib. Comput.*, vol. 67, no. 2, pp. 215–228, 2007.

[26] J. Mai, A. Sridharan, C.-N. Chuah, H. Zang, and T. Ye, "Impact of packet sampling on portscan detection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 12, pp. 2285–2298, Dec. 2006.

[27] F. Mattern and C. Floerkemeier, "From the Internet of computers to the Internet of Things," in *From Active Data Management to Event-Based Systems and More*, K. Sachs, I. Petrov, and P. Guerrero, Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 242–259.

[28] Y. Meng, L.-F. Kwok, and W. Li, "Towards designing packet filter with a trust-based approach using Bayesian inference in network intrusion detection," in *Proc. 8th Int. Conf. Secur. Privacy Commun. Netw. (SECURECOMM)*, 2012, pp. 203–221.

[29] Y. Meng, W. Li, and L.-F. Kwok, "Evaluation of detecting malicious nodes using Bayesian model in wireless intrusion detection," in *Proc. 7th Int. Conf. Netw. Syst. Secur. (NSS)*, 2013, pp. 40–53.

[30] Y. Meng, X. Luo, W. Li, and Y. Li, "Design and evaluation of advanced collusion attacks on collaborative intrusion detection networks in practice," in *Proc. 15th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Aug. 2016, pp. 1061–1068.

[31] W. Meng, W. Li, Y. Xiang, and K.-K. R. Choo, "A Bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks," *J. Netw. Comput. Appl.*, vol. 78, pp. 162–169, Jan. 2017.

[32] W. Meng, W. Li, and L.-F. Kwok, "Towards effective trust-based packet filtering in collaborative network environments," *IEEE Trans. Netw. Serv. Manage.*, vol. 14, no. 1, pp. 233–245, Mar. 2017.

[33] J. Mervis, "Agencies rally to tackle big data," *Science*, vol. 336, no. 6077, p. 22, 2012.

[34] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 48–60, Feb. 2004.

[35] P. Middleton, P. Kjeldsen, and J. Tully, "Forecast: The Internet of Things, worldwide, 2013," Gartner, Stamford, CT, USA, Tech. Rep. G00259115, 2013.

[36] A. Papadogiannakis, M. Polychronakis, and E. P. Markatos, "Improving the accuracy of network intrusion detection systems under load using selective packet discarding," in *Proc. EUROSEC*, 2010, pp. 1–7.

[37] P. A. Porras and R. A. Kemmerer, "Penetration state transition analysis: A rule-based intrusion detection approach," in *Proc. 8th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Nov./Dec. 1992, pp. 220–229.

[38] M. J. Probst and S. K. Kasera, "Statistical trust establishment in wireless sensor networks," in *Proc. Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2007, pp. 1–8.

[39] F. Wang, C. Huang, J. Zhang, and C. Rong, "IDMTM: A novel intrusion detection mechanism based on trust model for ad hoc networks," in *Proc. 22nd IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2008, pp. 978–984.

[40] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.

[41] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2006, pp. 640–644.

[42] R. A. Shaikh, H. Jameel, B. J. D'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[43] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 305–316.

[44] Y. Sun, H. Luo, and S. K. Das, "A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 9, no. 6, pp. 785–797, Nov. 2012.

[45] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[46] L.-B. Xu, G.-X. Wu, and J.-F. Li, "Packet-level adaptive sampling on multi-fluctuation scale traffic," in *Proc. Int. Conf. Commun., Circuits Syst.*, Hong Kong, May 2005, pp. 604–608.

[47] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 3, no. 3, pp. 366–379, Oct./Dec. 2004.

[48] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 69, no. 2, pp. 805–826, 2012.

[49] J. Zhang, R. Shankaran, M. A. Orgun, V. Varadharajan, and A. Sattar, "A dynamic trust establishment and management framework for wireless sensor networks," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Dec. 2010, pp. 484–491.

WEIZHI (YUXIN) MENG (M'10) received the B.Eng. degree in computer science from the Nanjing University of Posts and Telecommunications, China and the Ph.D. degree in computer science from the City University of Hong Kong (CityU), Hong Kong. He is currently an Assistant Professor with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark. He was a Research Scientist with the Infocomm Security Department, Institute for Infocomm Research, Singapore, and as a Senior Research Associate with CityU. He received the Outstanding Academic Performance Award during his doctoral study, and was a recipient of the HKIE Outstanding Paper Award for Young Engineers/Researchers in 2014 and 2017. He is also a co-recipient of the Best Student Paper Award from the 10th International Conference on Network and System Security in 2016. His primary research interests are cyber security and intelligent technology in security including intrusion detection, mobile security and authentication, HCI security, cloud security, trust computation, web security, malware, and vulnerability analysis. He also shows a strong interest in applied cryptography.

WENJUAN LI (S'15) is currently pursuing the Ph.D.degree with the Department of Computer Science, City University of Hong Kong (CityU), and holding a visiting position at the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark. She was a Research Assistant with CityU and was a Lecturer with the Department of Computer Science, Zhaoqing Foreign Language College, China. She was a recepient of Cyber Quiz and Computer Security Competition, Final Round of Kaspersky Laboratory Cyber Security for the Next Generation Conference in 2014. Her research interests include network management and security, collaborative intrusion detection, spam detection, trust computing, web technology, and E-commerce technology.

CHUNHUA SU received the B.S. degree from the Beijing Electronic and Science Institute in 2003, the M.S. and Ph.D. degrees in computer science from the Faculty of Engineering, Kyushu University, in 2006 and 2009, respectively. He is currently an Associate Professor with the Division of Computer Science, University of Aizu. From 2011 to 2013, he was a Research Scientist with the Cryptography and Security Department, Institute for Infocomm Research, Singapore. From 2013 to 2016, he was an Assistant Professor with the School of Information Science, Japan Advanced Institute of Science and Technology. From 2016 to 2017, he was Assistant Professor with the Graduate School of Engineering, Osaka University. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in data mining, and IoT security and privacy.

JIANYING ZHOU received the Ph.D. degree in Information Security from Royal Holloway, University of London. He was a Full Professor with the Singapore University of Technology and Design, and an Associate Center Director for iTrust. His research interests are in applied cryptography and network security, cyber-physical system security, and mobile and wireless security. He was a Principal Scientist and the Head of Infocomm Security Department, Institute for Infocomm Research, ASTAR. He has published over 200 referred papers at international conferences and journals with over 6000 citations, and received ESORICS'15 Best Paper Award. He also has two technologies being standardized in ISO/IEC 29192-4 and ISO/IEC 20009-4, respectively. He is a Co-Founder and the Steering Committee Co-Chair of ACNS. He is also the Steering Committee Chair of ACM Asia CCS and steering committee member of Asiacrypt. He has served over 200 times in international cyber security conference committees (ACM CCS and AsiaCCS, IEEE CSF, ESORICS, RAID, ACNS, Asiacrypt, PKC, FC.) as the General Chair, the Program Chair, and a PC member.

RONGXING LU (S'09–M'10–SM'15) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2012. He has been an Assistant Professor with the Faculty of Computer Science, University of New Brunswick (UNB), Canada, since 2016. From 2013 to 2016, he was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He was a Post-Doctoral Fellow with the University of Waterloo from 2012 to 2013. He received the most prestigious Governor General's Gold Medal, and received the 8th IEEE Communications Society (ComSoc) Asia Pacific Outstanding Young Researcher Award, in 2013. He is currently a Senior Member of the IEEE Communications Society. His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy. He has published extensively in his areas of expertise, and was the recipient (with his students and colleagues) of the Student Best Paper Award, ITS Summit Singapore 2015, the IEEE IES Student Best Paper Award 2014, the Best Paper Awards of Tsinghua Science and Technology Journal 2014, IEEE ICCC 2015, IEEE WCNC 2013, BodyNets 2010, and IEEE ICCCN 2009. He has been on the Editorial Boards of several international referred journals, such as, the IEEE Network, and served/serves the Technical Symposium Co-Chair of the IEEE Globecom'16, and many technical program committees of the IEEE and others international conferences, including the IEEE INFOCOM and ICC. He currently serves as the Secretary of IEEE Communications and Information Security Technical Committee. He is received the Excellence in Teaching Award, FCS, UNB of 2016–2017.