Detecting insider attacks in medical cyber–physical networks based on behavioral profiling

Meng, Weizhi; Li, Wenjuan; Wang, Yu; Au, Man Ho

Published in:
Future Generation Computer Systems

Link to article, DOI:
10.1016/j.future.2018.06.007

Publication date:
2020

Document Version
Peer reviewed version

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Detecting insider attacks in medical cyber–physical networks based on behavioral profiling☆

Weizhi Meng [a,b], Wenjuan Li [c], Yu Wang [a,*], Man Ho Au [d]

[a] School of Computer Science, Guangzhou University, China
[b] Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark
[c] Department of Computer Science, City University of Hong Kong, Hong Kong Special Administrative Region
[d] Department of Computing, The Hong Kong Polytechnic University, Hong Kong Special Administrative Region

HIGHLIGHTS

- A trust-based mechanism is built to detect insider nodes via behavioral profiling.
- We select four mobile and networking features to establish behavioral profiles.
- We apply Euclidean distance to derive a node's trust between two profiles.
- We performed evaluation by collaborating with a practical healthcare center.

ARTICLE INFO

Article history:
Received 3 January 2018
Received in revised form 19 March 2018
Accepted 2 June 2018
Available online xxxx

Keywords:
Medical cyber–physical system
Collaborative network
Intrusion detection
Trust management
Insider attack
Behavioral profiling

ABSTRACT

Cyber–physical systems (CPS) have been widely used in medical domains to provide high-quality patient treatment in complex clinical scenarios. With more medical devices being connected in industry, the security of medical cyber–physical systems has received much attention. Medical smartphones are one of the widely adopted facilities in the healthcare industry aiming to improve the quality of service for both patients and healthcare personnel. These devices construct an emerging CPS network architecture, called medical smartphone networks (MSNs). Similar to other distributed networks, MSNs also suffer from insider attacks, where the intruders have authorized access to the network resources, resulting in the leakage of patient information. In this work, we focus on the detection of malicious devices in MSNs and design a trust-based intrusion detection approach based on behavioral profiling. A node's reputation can be judged by identifying the difference in Euclidean distance between two behavioral profiles. In the evaluation, we evaluate our approach in a real MSN environment by collaborating with a practical healthcare center. Experimental results demonstrate that our approach can identify malicious MSN nodes faster than other similar approaches.

1. Introduction

Cyber–Physical Systems (CPS) integrates many entities including computational, networking, and physical processes. With the rapid development of digitalization technology in healthcare domains, medical CPS has become more inter- and intra-connected, but many of the used resources are the same as those employed by traditional enterprise IT (e.g., industrial applications, off-the-shelf technologies). In general, networked medical CPS can offer a plenty of benefits, i.e., achieving more efficient and less expensive monitoring and treatments. The integration among the embedded applications, the networking capabilities, and the complex physical dynamics of human body makes current medical device systems a unique CPS instance [2]. One report estimated that networked medical CPS technologies can save up to 63 billion in healthcare costs for the following fifteen years, reducing 15%–30% regarding medical equipment costs [3].

The major goal of medical CPS is to enhance the efficiency and effectiveness of patient care by ensuring personalized treatment in a safe way. As compared to a conventional network environment, medical CPS has the following two distinct features [4]. Firstly, the information communicated among medical devices is highly sensitive and private to both medical organizations and patient. For this sake, such sensitive data is a valuable target for cyber-criminals like making a profit. Secondly, the infrastructure

☆ A preliminary version of this paper appears in Meng et al. (2017) [1].

* Corresponding author.
E-mail addresses: weme@dtu.dk (W. Meng), yuwang@gzhu.edu.cn (Y. Wang).

https://doi.org/10.1016/j.future.2018.06.007
0167-739X/

of medical CPS is often complicated due to the large number and diversity of medical devices, especially Internet-enabled devices, which may be vulnerable to a broader range of cyber threats [5]. For instance, the number of information security breaches reported by healthcare providers had an increase of 60% from 2013 to 2014, where the increase rate is only 30% in other industries [6]. As medical industry is evolving rapidly, the security of medical CPS should be given much more attention [7].

Motivations. Due to the increasing capabilities, mobile devices have been widely used to carry information and speed up electronic data transfers. Currently, medical smartphones are available in various healthcare organizations, assisting the record of patient's medical conditions and the organization of patient's records in real-time. Subsequently, an emerging medical network infrastructure has been initialized, called *medical smartphone network (MSN)* [8]. These phones can connect with each other as well as the organization's network. The recent McAfee report indicates that Internet-enabled medical devices may expose security gaps in the integration of operational technology, consumer technology and networked information technology [9]. Due to the distributed nature, MSNs are vulnerable to insider attacks, in which an intruder can access the resources within the network. Without timely detection, insider attacks can cause a network to be paralyzed. Therefore, there is a need for defending MSNs against various attacks, especially insider threats (i.e., each medical device can be considered as a network node).

Contributions. Because of the importance and sensitivity of MSNs, it is crucial to identify malicious devices within such network in a quick manner. Previous studies (e.g., [8]) has shown that trust-based intrusion detection systems (IDSs) are a promising solution. Motivated by this observation, in this work, we develop a trust-based intrusion detection mechanism for MSNs to identify malicious MSN nodes in a fast manner, based on the Euclidean distance between the current profile and the normal profile. The contributions can be summarized as below.

- To facilitate the understanding of MSNs, we describe the hierarchical infrastructure of MSNs that is often adopted in a medical network environment. We also introduce the basic MSN features and the requirements from healthcare managers regarding the design of a desirable security mechanism.
- We design a trust-based intrusion detection mechanism that identifies malicious MSN nodes by comparing behavioral profiles. A behavioral profile represents a collection of necessary information to describe the basic characteristics of an object under pre-defined rules. Further, based on the suggestions from healthcare managers, we select four mobile and network features to build behavioral profiles, and apply Euclidean distance for evaluating a node's reputation.
- By collaborating with a healthcare center, we evaluate the performance of our proposed mechanism in a real MSN environment. Experimental results demonstrate that our mechanism is effective at identifying malicious MSN nodes in a faster manner than other similar approaches, with a reasonable workload in practical setup.

The remaining parts of this paper are organized as follows. In Section 2, we present relevant research studies on the application of trust-based intrusion detection mechanisms in detecting insider attacks. Section 3 introduces the background of MSNs and describes our designed mechanism in detail, including how to build a behavioral profile based on the selected features and how to calculate a node's reputation in terms of Euclidean distance. Section 4 describes experimental settings and discusses our evaluation results. Finally, Section 5 concludes our work.

2. Related work

Insider attacks are one of the major threats for distributed systems, where the malicious point within the network has legitimate access to computer resources. For example, a malicious node in a wireless sensor networks (WSNs) can spread untruthful information to other nodes. To identify adversarial nodes in a distributed network, the key issue is how to build trust among various nodes. In literature, trust-based IDSs are often used to defend against insider threats through evaluating the trustworthiness of a node in an active and appropriate way.

Distributed or collaborative trust-based intrusion detection. To enhance the detection performance of a single IDS, collaborative intrusion detection networks (CIDNs) were proposed, enabling an IDS node to gather required information with other IDS nodes [10]. Many distributed intrusion detection systems usually adopted a centralized architecture with centralized fusion or distributed fusion [11–14]. For instance, Li et al. [15] proposed a distributed IDS, which was built based on the emerging decentralized location and routing infrastructure. Their results showed a better performance than the traditional hierarchical approach when facing large amounts of diverse intrusion alerts. However, their approach assumed that all peers are trusted, which is vulnerable to insider attacks (i.e., betrayal attacks where some nodes suddenly become malicious).

To detect malicious insider nodes, Duma et al. [16] presented a P2P-based overlay IDS aiming to mitigate malicious insider threat by means of both a trust-aware engine for correlating alerts and an adaptive scheme for managing trust. The correlation engine could help filter out warnings sent by untrusted or low quality peers, and the adaptive scheme could predict a node's reputation based on the past experiences. Shaikh et al. [17] proposed GTMS, a Group-based Trust Management Scheme that could evaluate the trustworthiness under two topologies: namely, intra-group topology and inter-group topology. Zhang et al. [18] designed a dynamic trust management framework for hierarchical networks, by combining both direct and indirect (group) trust for reputation computation. They further assigned more weight to the most recently obtained trust values to erase any negative impact. Guo et al. [19] developed a trust management framework that used grey theory and fuzzy sets to predict trust for a node. The trust values could be calculated by considering both relation factors and weights of neighbor nodes, not just by simply taking an average value. Some other related work regarding can be referred to [20–23].

Challenge-based intrusion detection mechanism (shortly challenge mechanism). This is a special method of managing trust, in which a node can send challenges to evaluate the trustworthiness of other nodes. The reputation can be derived by comparing the received answers with the challenges. Fung et al. [24] developed a challenge-based collaboration framework to evaluate the trustworthiness among host-based IDS nodes. They also used a forgetting factor, which could give more emphasis on the recent feedback of the target nodes. To leverage the use of mutual experience, they gave an improved trust management model by adopting a Dirichlet-based model to measure the level of trustworthiness among a set of IDS nodes [25]. The improved model had strong scalability properties and experimental results demonstrated that its robustness and efficiency.

However, such challenge mechanism may be vulnerable to advanced insider attacks, Li et al. [26] developed an advanced collusion attack, called *passive message fingerprint attack* (PMFA), enabling malicious nodes to maintain their trust while sending untruthful responses to normal requests. Meng et al. [27] also identified that challenge mechanisms would be not realistic due to some assumptions and may lead to a weak threat model in

Please cite this article in press as: W. Meng, et al., Detecting insider attacks in medical cyber–physical networks based on behavioral profiling, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.06.007.

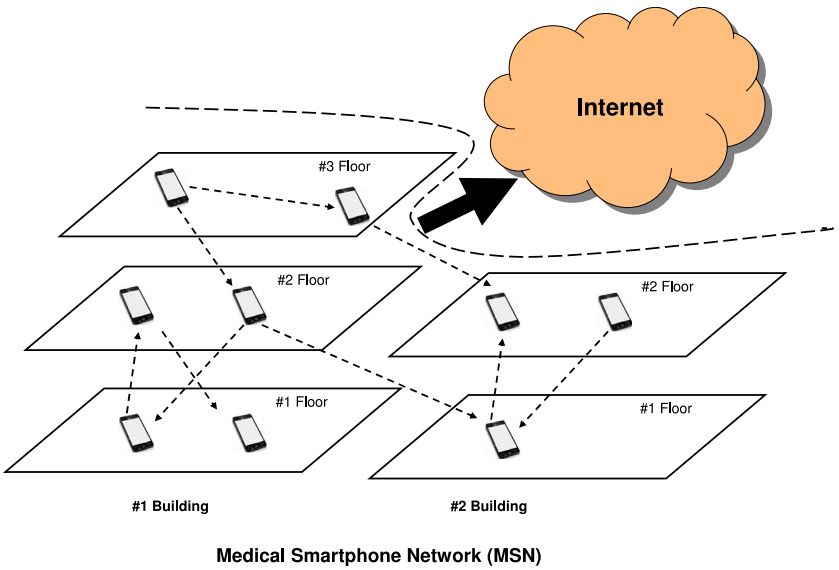


Fig. 1. The typical architecture of medical smartphone networks (MSNs).

practical scenarios. They then designed an advanced collusion attack, called *random poisoning attack*, which can enable a malicious node to send untruthful information without decreasing its trust value at large. Li et al. [28] further designed a special on–off attack, where a malicious node could send truthful answers to one node but behave untruthfully to another node. Such attack may affect the trust computation in a third node.

To improve the performance of challenge mechanisms, Li et al. [29] found that different IDSs may have different levels of sensitivity in detecting particular types of intrusions based on their own signatures and settings. They then defined a notion of *intrusion sensitivity* and designed a trust management model to improve the robustness of CIDNs [30]. They further proposed a machine learning-based approach in automatically allocating the values of *intrusion sensitivity* in real-world applications [31]. Several other related studies regarding IDS improvement can be referred to [32–43].

As MSNs are an emerging medical network infrastructure, there have been few studies on the identification of malicious nodes in this environment [1]. Motivated by this, our work proposes a trust-based intrusion detection approach to help detect malicious MSN insider nodes based on behavioral profiling. Our work aims to complement existing security mechanisms in healthcare domains and stimulate more research in this field.

3. Our approach

In this section, we introduce the background of MSNs and illustrate how to defend MSNs against insider attacks based on behavioral profiling-based trust management.

3.1. Background on MSNs

Thanks to various add-ons and applications, existing smartphones can provide many benefits for the diagnosis and treatment of patient (i.e., counting calories and measuring heartbeats) [44]. With this revolution, these medical smartphones construct an emerging network architecture, called medical smartphone networks (MSNs), which have been gradually adopted in many healthcare organizations such as hospitals, clinics and healthcare centers. Fig. 1 depicts a typical architecture of MSNs.

Fig. 1 shows that medical smartphones connect with each other within the same network, aiming to facilitate information exchange and patient management. A medical device (or node) in MSNs can also access the resources from the Internet. The networked devices embed the Internet into patients' lives, improve medical outcomes and lower healthcare costs [8]. However, due to the sensitive information exchanged and stored in such environment, cyber-criminals are very likely to compromise such type of network for profits.

Insider attacks are one of the big threats for this distributed network infrastructure. For example, an attacker can lurk inside the healthcare organizations and physical access to the phones or infect them through Wifi, bluetooth, or other tools. As long as one MSN node is compromised, then the attacker can attack other nodes via adversarial tools such as scanning, spoofing, denial-of-service (DoS) attacks and so on. In other words, insider attacks can significantly leak sensitive information and even cause the paralysis of the entire network. Thus, there is a great need to identify malicious MSN nodes in a fast manner for protecting patient's sensitive information and securing the network operations.

Challenges on MSNs. According to a recent study [8], most healthcare managers considered that MSNs are different from conventional wireless network architecture, and have its unique challenges.

- *Lack of IT experts.* The security of medical devices are often maintained by manufacturers, due to the lack of IT experts in a healthcare organization. However, IT experts are becoming more important with more medical devices start to connect to the Internet. This makes the traffic in a MSN become more complicated than before. For example, medical devices containing configurable embedded computer systems may be vulnerable to cyber security breaches.
- *Risk management.* As most healthcare workers are not IT experts, they are unfamiliar with handling cyber attacks. For example, they cannot identify whether the medical phones are infected by virus or not, delaying the detection of malicious devices. This makes centralized control and management essential in designing a security mechanism for MSNs.

Due to these challenges, it is critical to design appropriate security mechanisms to protect MSNs against insider attacks. More specifically, healthcare managers gave the following two suggestions, according to [8].

Please cite this article in press as: W. Meng, et al., Detecting insider attacks in medical cyber–physical networks based on behavioral profiling, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.06.007.

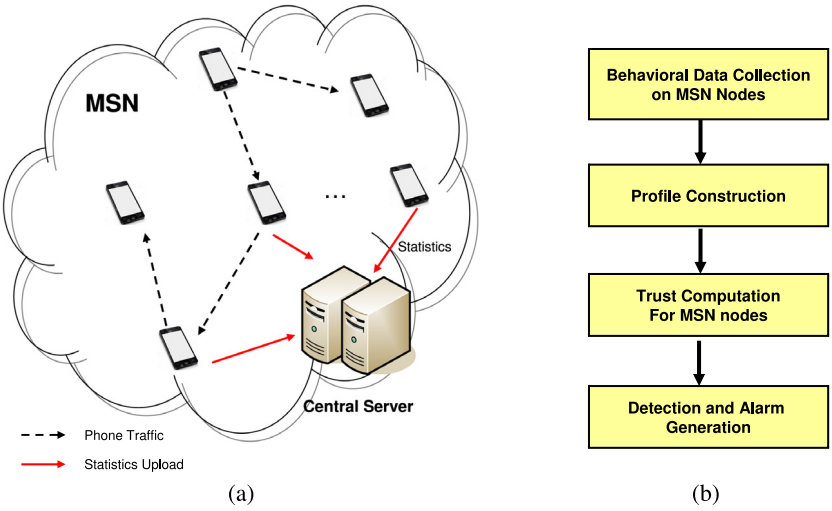


Fig. 2. (a) The high-level architecture of our mechanism; and (b) typical detection flows.

- A centralized architecture is desirable for detecting malicious nodes in MSNs, as healthcare organizations are often short of IT-trained personnel. Due to this, centralized or hierarchical security mechanisms can help reduce the number of potential attack vectors.
- To enable networked medical devices to operate effectively and smoothly, healthcare organizations prefer the deployed mechanisms to identify malicious nodes in a dynamic manner with fault tolerance (i.e., reducing false positives).

Overall, an ideal mechanism should be able to support full-time management for inspecting traffic and applying appropriate security policies to respond to accidents.

3.2. Trust-based intrusion detection architecture

As explained above, healthcare managers expect to deploy a hierarchical security mechanism to protect MSNs against insider attacks. Fig. 2 shows the high-level architecture and the detection workflows of our proposed trust-based intrusion detection mechanism.

- Fig. 2(a) details the hierarchical trust-based intrusion detection mechanism, where the central server is responsible for collecting behavioral data from IDS nodes. In real-world applications, each MSN node deploys a lightweight IDS agent for inspecting traffic and sending data to the central server periodically.
- Fig. 2(b) illustrates the major detection flows including *behavioral data collection*, *profile construction*, *trust computation for MSN nodes*, and *detection and alarm generation*. The collection of behavioral data is an important step for building a robust trust-based intrusion detection scheme. The gathered data can be used to build a normal behavioral profile for a MSN node. Then, a node's trustworthiness can be evaluated through identifying the deviations between historical profile and current profile. If the trust value of a node is lower than a pre-defined threshold, then an alarm will be generated to alert security administrators.

3.3. Behavioral profiling and feature selection

A behavioral profile is a collection of required information with the purpose of representing the characteristics of an object under pre-defined rules. For instance, a business card can contain a set of basic features like name, department and business phone number. In literature, it has been proved to be an effective solution to model a target [45]. To create a stable behavioral profile, there is a need for using sensible specifications to define the behavior.

Table 1
Basic features of smartphone users.

Outgoing calls	Incoming calls	Video calls
Location	Time	SMS
Favorite websites	Email address	IP of access points
Bluetooth ID	Camera usage	Application usage
Keystroke	Downloaded files	Media player usage

Generally, many basic features can be extracted when users are using their phones, such as phone calls (including outgoing, incoming and video), location, timing information, Short Message Service (SMS), visited websites, Email address, application usage, and so on. A set of basic features is summarized in Table 1. While a balance should be made to decide what kind of data can be collected for MSNs, due to its specialty and requirements (i.e., healthcare organizations would not want to disclose all data to third-parties). In this work, we collaborated with a healthcare center and based on their professional suggestions, we select the following daily features to construct a behavioral profile for MSN nodes.

- *Camera usage.* As medical records are extremely sensitive, camera usage should be given more attention, i.e., when the camera application is used.
- *Visited websites.* If a node is infected by malware or virus, it is very likely to open and visit certain websites to download or upload data, i.e., which kinds of websites are visited during a period of time.
- *Short message service (SMS) usage.* If a node is compromised, SMS can be used to leak sensitive information. Thus, SMS usage should be considered in practice, i.e., when the messages are sent.
- *Email address.* Similarly, sending or receiving Emails is a kind of sensitive event as well, which can be a target for phishing websites and ransomware.

To quantify behavior patterns into concrete metrics, based on the suggestions from the collaborated healthcare organizations, we devise a quantification scheme for each selected feature as below.

Please cite this article in press as: W. Meng, et al., Detecting insider attacks in medical cyber–physical networks based on behavioral profiling, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.06.007.

- *Camera usage.* This metric is defined as a 24-element vector, with each element corresponds to one hour for the day. The value of each element is the empirical probability a device uses the camera application.
- *Visited websites.* This metric is defined as a 2-element vector, with each element corresponds to one type of websites: normal website and unknown website. A healthcare organization often defines a list of whitelisted websites; thus, we can classify normal website and unknown websites accordingly. The value of each element is the empirical probability a device visits the relevant websites.
- *Short message service.* This metric is defined as a 24-element vector, with each element corresponds to one hour for the day. The value of each element is the empirical probability a device uses SMS.
- *Email address.* This metric is defined as a 4-element vector, with each element corresponds to one type of email addresses: normal sender, unknown sender, normal recipient and unknown recipient. The classification can also be done via a whitelist. The value of each element is the empirical probability a device uses the email service.

3.4. Euclidean distance-based trust computation

To evaluate the trustworthiness of a MSN node, we have to identify the difference between two behavioral profiles. If given any two profiles, say $P1$ and $P2$, and corresponding vectors $A = (a_1, a_2, \ldots, a_n)$ and $B = (b_1, b_2, \ldots, b_n)$, then the corresponding Euclidean distance can be computed as below:

$$E(A, B) = \sqrt{\sum_{i=1}^{n}(a_i - b_i)^2}. \quad (1)$$

In this work, we consider four major sectors: camera usage, visited websites, SMS and Email address. Thus, the difference between two behavioral profiles can be calculated by taking the Euclidean norm of the Euclidean distance vector [45], as below:

$$D(P1, P2) = \sqrt{\sum_{j=1}^{4}(E_j)^2}. \quad (2)$$

The resulting value ($\in [0, 2]$) is the difference of the two behavioral profiles. It is worth noting that a larger value indicates a more significant difference between two profiles. Based on the use of Euclidean distance, the trustworthiness of a MSN node can be computed as follow.

$$t^d_{value} = 1 - \frac{D(P1, P2)}{2} \quad (3)$$

where t^d_{value} indicates the trust value of node d and $\frac{D(P1,P2)}{2}$ aims to normalize the range of $D(P1, P2)$ to [0, 1]. Subsequently, a node's trustworthiness can be computed using the above equation and a malicious node can be determined by setting a trust threshold. Let τ denote the trust threshold, then we can judge whether a node is malicious as below:

- If $t^d_{value} \geq \tau$, then the node is considered as a normal node.
- If $t^d_{value} < \tau$, then the node is regarded as a malicious (or untruthful) node.

In practice, a trade-off should be made between false negative rate and false positive rate. Malicious nodes can be handled depending on the specific security policies defined by the organization. Therefore, IT administrators in the healthcare organizations can have enough flexibility to control and manage the whole network.

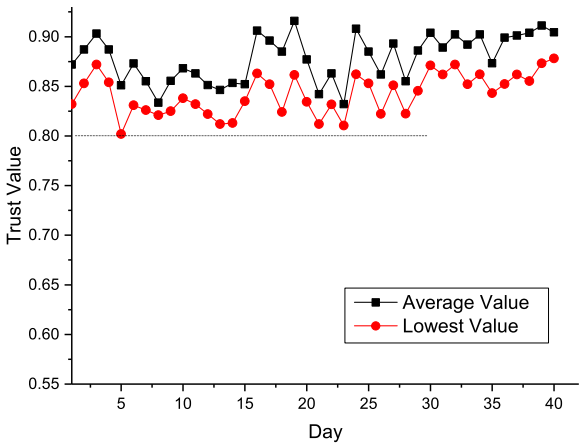


Fig. 3. The trend of trust values under normal MSN environment with 25 nodes.

4. Evaluation

In this section, we collaborated with a healthcare center located in South China (with around 100 personnel) to investigate the performance of our proposed approach. Due to privacy concerns, our mechanism was implemented in a MSN environment, including 25 nodes. A central server was deployed to collect required data from each node and was responsible for computing their trust values (see Fig. 2(a)). The server was composed of an Intel(R) Core (TM)2, Quad CPU 2.66 GHz. Further, the healthcare manager defined 76 normal websites, 107 Email senders and 101 recipients based on its historical data and current network settings. We mainly conduct two experiments:

- *Experiment-1.* This experiment aims to observe the trend of nodes's trust values in a normal MSN environment and identify an appropriate threshold that can be used to detect anomalies.
- *Experiment-2.* This experiment investigates the effectiveness of our mechanism under adversarial scenarios, where some nodes would behave untruthfully (i.e., breaking the defined policies).

4.1. Experiment-1

It is worth noting that a larger t^d_{value} means that a node is more credible. Ideally, t^d_{value} is expected to reach 1; however, it was not realistic in real-world scenarios. Thus, the major purpose of this experiment is to identify an appropriate threshold that can be used to detect malicious nodes in MSNs. In this experiment, we observed the trend of trust values in a normal MSN environment for 40 days. Fig. 3 depicts the trend of average and lowest trust value during the experiment.

The average trust value is an average value including all MSN nodes within the network, which is able to reflect the overall network performance, while the lowest trust value indicates the worst node's reputation. Fig. 3 shows that the average trust value was generally higher than 0.825, and the lowest trust value was ranged from 0.8 to 0.878. Since there is no update for MSN nodes' normal profiles, we consider that the behavioral profiles are relatively stable in the deployed healthcare environment.

To validate the threshold, we deployed our mechanism in another MSN environment with 35 nodes. As shown in Fig. 4, it is found that the trend of trust values is similar to Fig. 3, i.e., the lowest trust value is higher than 0.8 in the normal MSN environment. In this case, we choose 0.8 as the trust threshold for the deployed environment.

Please cite this article in press as: W. Meng, et al., Detecting insider attacks in medical cyber–physical networks based on behavioral profiling, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.06.007.

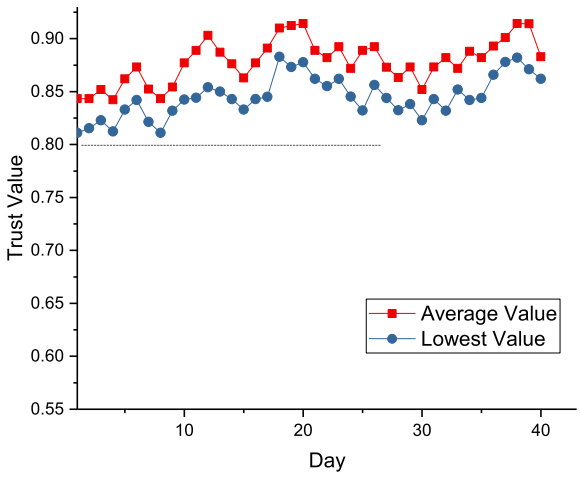


Fig. 4. The trend of trust values under normal MSN environment with 35 nodes.

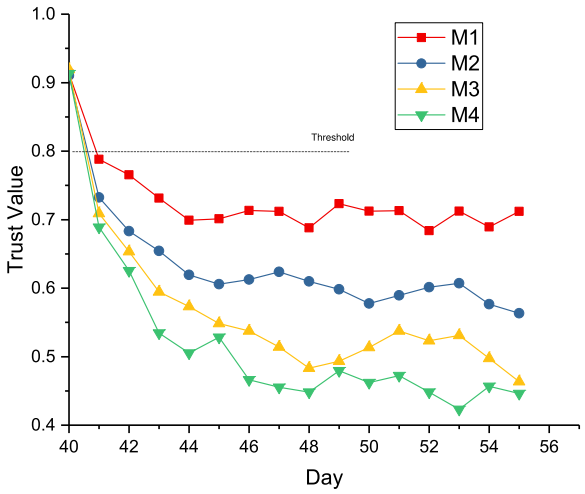


Fig. 5. The trust values of malicious nodes: *M1*, *M2*, *M3* and *M4*.

Table 2
Simulated unusual events for each malicious nodes.

Node	Camera	Visited websites	SMS	Email address
M1	√	–	–	–
M2	√	√	–	–
M3	√	√	√	–
M4	√	√	√	√

4.2. Experiment-2

In this experiment, we aim to investigate the practical performance of our approach under an adversarial scenario, where some MSN nodes behaved maliciously. In particular, we randomly selected four nodes (named *M1*, *M2*, *M3* and *M4*) as malicious to launch insider attacks, i.e., visiting unusual websites, or sending Emails to undefined recipients. Table 2 summarizes the unusual events for each malicious node, in which *M1* only violated one sector, *M2* violated the sectors of camera usage and website visits, *M3* broke three sectors and *M4* behaved untruthfully for all sectors. Following the first experiment, malicious events were started from Day 41. The trust values of malicious nodes are depicted in Fig. 5.

- From Day 41, it is observed that the trust values of malicious nodes could decrease below the threshold of 0.8 in a fast manner. The trust value of *M1*, *M2*, *M3* and *M4* ranged from 0.688 to 0.788, from 0.563 to 0.733, from 0.463 to 0.708, and from 0.423 to 0.688, respectively.
- Fig. 5 also showed that the trust value of *M4* decreased more quickly than others, whereas the trust value of *M1* decreased the slowest. This is because *M4* violated more sectors than the other malicious nodes, while *M1* only violated one sector.

To our knowledge, there have been few studies regarding the identification of insider attacks for MSNs. Meng and Au [46] proposed a statistical trust computation based on behavioral profiling, which is the most relevant work. For example, if there are two out of ten events and one out of eight events are malicious for a node, then the node's trust value can be computed as $(1 - 2/10 * 1/8 =)$ 0.975. Fung et al. [24,25] developed a challenge-based trust management model for identifying malicious nodes in a collaborative network. To facilitate the comparison, we tuned this model to fit a hierarchical structure, i.e., a central server was deployed for data collection and trust computation.

To launch insider attacks, we randomly selected four nodes to behave untruthfully according to Table 2. The average trust value of malicious nodes is shown in Fig. 6. We have the following major observations.

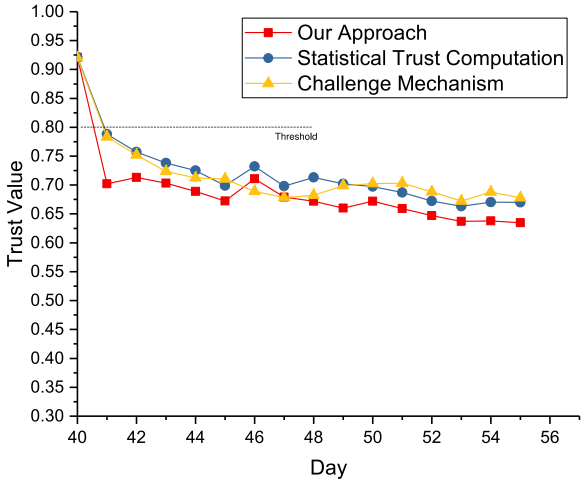


Fig. 6. A comparison of average trust value of malicious nodes under different trust management approaches.

- Our approach could decease the trust values of malicious nodes faster than other two approaches. For example, our approach could reduce the reputation level to nearly 0.702 on Day 41, whereas the other approaches could only decrease the trust value to approximately 0.788 on Day 41.
- Among the three approaches, it is found that the trend of trust values was more smooth under the challenge mechanism. This is because a forgetting factor was used to consider the older behavioral events but highlight the recent sectors.

To validate the performance, we randomly selected four different nodes to behave maliciously based on Table 2. The average trust value of malicious nodes is depicted in Fig. 7. Similarly, it is found that our approach still achieved the best detection performance among the three approaches, i.e., our approach can reduce the trust values of malicious nodes to 0.73. while the other two could only reduce the reputation level to 0.77. These results validate that our approach could reduce the trust values of malicious nodes more quickly than similar approaches.

To summarize, the experimental results demonstrate that our mechanism is more effective to detect malicious MSN nodes than

Please cite this article in press as: W. Meng, et al., Detecting insider attacks in medical cyber–physical networks based on behavioral profiling, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.06.007.

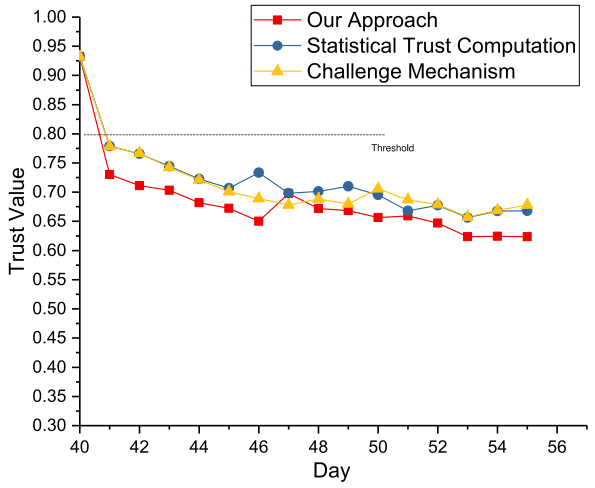


Fig. 7. A validation of reputation level of malicious nodes under different trust management approaches.

Table 3
CPU workload for central server and MSN nodes under different scenarios.

Central server side Condition	Average CPU (%)	Max CPU (%)
Normal scenario	11.8	18.7
Adversarial scenario	20.4	33.2
MSN node side Condition	**Average CPU (%)**	**Max CPU (%)**
Normal scenario	5.6	8.7
Adversarial scenario	10.6	16.5

the other two similar approaches (i.e., decreasing the trust value of malicious nodes in a faster manner). Our observations were also confirmed by IT administrators in the participating healthcare organization.

4.3. Workload

Intuitively, deploying extra trust management mechanisms would cause additional CPU load on both central server side and phone side, due to communication and operation cost. On the central server side, workload is mainly caused by operations such as collecting profile information, computing reputation for each MSN node, exchanging commands with nodes, and so on. On the phone side, workload is caused by operations like monitoring phone applications, collecting behavioral events and uploading data to the server, etc.

Table 3 presents the CPU workload for both central server and MSN nodes under normal and adversarial scenarios in the deployed healthcare environment. We have the following major observations.

- Intuitively, the central server's workload was heavier than the node side. Under the normal environment, the workload ranged from 11.8% to 18.7%, and from 5.6% to 8.7% for the central server and MSN nodes, respectively. This is because the server has to collect information, compute trust values for MSN nodes, and detect untruthful nodes.
- Under the adversarial environment, an increase of workload was observed for both server and node side, i.e., under insider attacks, the server's maximum workload could increase to 33.2% (with an average of 20.4%), and the average workload for MSN nodes was increased from 5.6% to 10.6%. This is because more malicious behavioral events would increase the communication frequency between server and node side.

The reported workload has included all operations in addition to those operations required by our proposed mechanism. By considering the actual workload required by most healthcare facilitates, healthcare IT administrators believed that the CPU workload used by our mechanism is applicable and reasonable.

4.4. Discussion

Behavioral profile. In this work, we mainly consider four features to build a behavioral profile based on the advice from the healthcare mangers. Undoubtedly, combining more features may help establish a more precise profile for MSNs. However, there is a need to develop a robust security scheme with few features, as medical network is extremely sensitive in which some expected features may be not available in some cases (i.e., due to the availability and privacy concerns in healthcare domain). This is an open challenge in this area.

Detection threshold. The trend of trust values depicted in our work validates that behavioral profile of a MSN node is more stable, indicating that the traffic in a medical network would be not as dynamic as a conventional network. Thus, a well-defined normal profile can be effective for a long period. However, it is still an interesting topic to investigate the performance and the threshold by updating the normal profile periodically. In addition, one of our future directions is to develop compact and effective security schemes for saving energy and storage in resource-limited medical devices.

Feature selection. In this work, we mainly considered four features medical phones, including camera usage, visited websites, SMS, and Email address, as these features were preferred by the healthcare managers and it is easier to get the data from the participating healthcare organization. In practice, there are many alternatives such as phone calls (including outgoing, incoming and video), location, timing information and application types, and so on. One of our future work is to investigate the impact of other available behavioral features on the detection performance.

Trust computation. In this work, trustworthiness of a node is derived through identifying the difference between two profiles using Euclidean distance. Though a node's behavioral profile is relatively stable in the MSN environment, there is a need to build a more accurate profile by considering *variance*. This is a challenge and one of our future directions.

Forgetting factor. As observed in our evaluation, challenge mechanism [24] employed a forgetting factor to give more weight on recent behavioral events. This factor can be applied in our future studies aiming to make the trend of trust values smooth.

Performance improvement. In literature, Meng et al. [8] presented a trust management approach to detect MSN insider attacks based on traffic inspection, but it is not fair to compare it with our mechanism. This is because the trust computation adopts different resources: one is network traffic while the other is behavioral event. However, it is an interesting topic to investigate the performance of combining these two approaches.

5. Conclusion

With more devices inter- and Internet-connected, medical smartphone networks (MSNs) have emerged as a popular architecture in various healthcare organizations. Due to the distributed nature, MSNs are still vulnerable to insider attacks. In this work,

Please cite this article in press as: W. Meng, et al., Detecting insider attacks in medical cyber–physical networks based on behavioral profiling, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.06.007.

we focus on MSNs and propose a hierarchical trust-based intrusion detection mechanism based on behavioral profiling. The trustworthiness of MSN nodes can be derived by identifying the difference in Euclidean distance between two behavioral profiles. By collaborating with a practical healthcare center, we explored the performance of our mechanism in a real MSN environment. Experimental results demonstrate that our mechanism is effective in detecting malicious MSN nodes in a faster manner, than the other similar approaches.

There are many possible topics for future work, which include investigating how to efficiently identify a trust threshold in different network environments. It is also an interesting topic to consider more features in trust computation and explore the application of forgetting factors.

Acknowledgments

This work was partially supported by National Natural Science Foundation of China (No. 61472091), Natural Science Foundation of Guangdong Province, China for Distinguished Young Scholars (2014A030306020), Science and Technology Planning Project of Guangdong Province, China (2015B010129015) and the Innovation Team Project of Guangdong Universities, China (No. 2015KCXTD014).

References

[1] W. Meng, W. Li, Y. Wang, M.N. Au, Detecting Malicious Nodes in Medical Smartphone Networks through Euclidean Distance-based Behavioral Profiling, in: Proceedings of the 9th International Symposium on Cyberspace Safety and Security (CSS 2017), 2017, pp. 163–175.

[2] R. Rajkumar, D.de. Niz, M. Klein, Medical Cyber-Physical Systems.http://www.informit.com/articles/article.aspx?p=2756464.

[3] P.C. Evans, M. Annunziata, Industrial Internet, Pushing the Boundary of Mind and Machines. (November, 2012) Available at: http://www.ge.com/sites/default/files/Industrial_Internet.pdf.

[4] Symantec, Networked Medical Devices: Security and Privacy Threats. (June 2015) Available at: https://www.symantec.com/content/en/us/enterprise/white_papers/b-networked_medical_devices_WP_21177186.en-us.pdf..

[5] P.A.H. Williams, A.J. Woodward, Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem, Medical Devices: Evidence and Research 8 (2015) 305–316.

[6] P. Harries, The Prognosis for Healthcare Payers and Provider- s: Rising Cybersecurity Risks and Costs. (December, 2014) Available Online at: http://usblogs.pwc.com/cybersecurity/the-prognosis-for-healthcare-payers-and-providers-rising-cybersecurity-risks-and-costs/.

[7] W. Meng, L. Jiang, Y. Wang, J. Li, J. Zhang, Y. Xiang, JFCGuard: detecting juice filming charging attack via processor usage analysis on smartphones, in: Computers & Security, Elsevier, 2018 (in press).

[8] W. Meng, W. Li, Y. Xiang, K.K.R. Choo, A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks, J. Netw. Comput. Appl. 78 (2017) 162–169.

[9] J. Healey, N. Pollard, B. Woods, The Healthcare Internet of Things: Rewards and Risks. (March 2015) Available Online at: http://www.mcafee.com/mx/resources/reports/rp-healthcare-iot-rewards-risks.pdf.

[10] Y.-S. Wu, B. Foo, Y. Mei, S. Bagchi, Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS, in: Proceedings of the 2003 Annual Computer Security Applications Conference (ACSAC), 2003, pp. 234–244.

[11] B. Chun, J. Lee, H. Weatherspoon, B.N. Chun, Netbait: a Distributed Worm Detection Service. Technical Report IRB-TR-03-033, Intel Research Berkeley, 2003.

[12] R. Huebsch, B.N. Chun, J.M. Hellerstein, B.T. Loo, P. Maniatis, T. Roscoe, S. Shenker, I. Stoica, A.R. Yumerefendi, The Architecture of PIER: an Internet-Scale Query Processor, in: Proceedings of the 2005 Conference on Innovative Data Systems Research (CIDR), 2005. pp. 28–43.

[13] P.A. Porras, P.G. Neumann, Emerald: Event Monitoring Enabling Responses to Anomalous Live Disturbances, in: Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 353–365.

[14] S.R. Snapp, et al. DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype, in: Proceedings of the 14th National Computer Security Conference, 1991, pp. 167–176.

[15] Z. Li, Y. Chen, A. Beach, Towards Scalable and Robust Distributed Intrusion Alert Fusion with Good Load Balancing, in: Proceedings of the 2006 SIGCOMM Workshop on Large-Scale Attack Defense (LSAD), 2006. pp. 115–122.

[16] C. Duma, M. Karresand, N. Shahmehri, G. Caronni, A Trust-Aware, P2P-Based Overlay for Intrusion Detection, in: Proccedings of DEXA Workshop, 2006, pp. 692–697.

[17] R.A. Shaikh, H. Jameel, B.J. d'Auriol, H. Lee, S. Lee, Y.J. Song, Group-based trust management scheme for clustered wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 20 (11) (2009) 1698–1712.

[18] J. Zhang, R. Shankaran, M.A. Orgun, V. Varadharajan, A. Sattar, A Dynamic Trust Establishment and Management Framework for Wireless Sensor Networks, in: Proceedings of the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC), 2010, pp. 484–491.

[19] J. Guo, A. Marshall, B. Zhou, A New Trust Management Framework for Detecting Malicious and Selfish Behaviour for Mobile Ad Hoc Networks, in: Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011. pp. 142–149.

[20] K. Daabaj, M. Dixon, T. Koziniec, K. Lee, (2010) Trusted Routing for Resource-Constrained Wireless Sensor Networks, in: Proceedings of the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC), 2010, pp. 666–671.

[21] C.A. Kerrache, N. Lagraa, C.T. Calafate, A. Lakas, TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs, Veh. Commun. 9 (2017) 254–267.

[22] W. Meng, W. Li, C. Su, J. Zhou, R. Lu, Enhancing trust management for wireless intrusion detection via traffic sampling in the Era of Big Data, IEEE Access 6 (2018).

[23] G. Rajeshkumar, K.R. Valluvan, An energy aware trust based intrusion detection system with adaptive acknowledgement for wireless sensor network, Wirel. Pers. Commun. 94 (4) (2017) 1993–2007.

[24] C.J. Fung, O. Baysal, J. Zhang, I. Aib, R. Boutaba, Trust Management for Host-Based Collaborative Intrusion Detection, in: Proceedings of DSOM, LNCS 5273, 2008. 109–122.

[25] C.J. Fung, J. Zhang, I. Aib, R. Boutaba, Robust and scalable trust management for collaborative intrusion detection, in: Proceedings of the 11th IFIP/IEEE International Conference on Symposium on Integrated Network Management (IM), 2009, pp. 33–40.

[26] W. Li, W. Meng, L.F. Kwok, H.H.S. Ip, PMFA: Toward Passive Message Fingerprint Attacks on Challenge-based Collaborative Intrusion Detection Networks, in: Proceedings of the 10th International Conference on Network and System Security (NSS), 2016, pp. 433–449.

[27] W. Meng, X. Luo, W. Li, Y. Li, Design and Evaluation of Advanced Collusion Attacks on Collaborative Intrusion Detection Networks in Practice. in: Proceedings of the 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2016. pp. 1061–1068.

[28] W. Li, W. Meng, L.F. Kwok, SOOA: Exploring Special On-Off Attacks on Challenge-based Collaborative Intrusion Detection Networks. in: Proceedings of the 12th International Conference on Green, Pervasive and Cloud Computing (GPC 2017), 2017, pp. 402–415.

[29] W. Li, Y. Meng, L.F. Kwok, Enhancing Trust Evaluation Using Intrusion Sensitivity in Collaborative Intrusion Detection Networks: Feasibility and Challenges, in: Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS), 2013. pp. 518–522.

[30] W. Li, W. Meng, L.F. Kwok, Design of Intrusion Sensitivity-Based Trust Management Model for Collaborative Intrusion Detection Networks, in: Proceedings of the 8th IFIP WG 11.11 International Conference on Trust Management (IFIPTM), 2014. pp. 61–76.

[31] W. Li, W. Meng, L.F. Kwok, H.H.S. Ip, Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model, J. Netw. Comput. Appl. 77 (2017) 135–145.

[32] H. Bostani, M. Sheikhan, Hybrid of anomaly-based and specification-based IDS for internet of things using unsupervised OPF based on MapReduce approach, Comput. Commun. 98 (2017) 52–71.

[33] J. Li, L. Sun, Q. Yan, Z. Li, H. Ye, Witawas Srisa-an, Significant permission identification for machine learning based android malware detection, IEEE Trans. Ind. Inf. (2018) (in press).

[34] J. Li, Y. Zhang, X. Chen, Y. Xiang, Secure attribute-based data sharing for resource-limited users in cloud computing, Comput. Secur. 72 (2018) 1–12.

[35] W. Li, W. Meng, L.F. Kwok, H.H.S. Ip, Developing Advanced Fingerprint Attacks on Challenge-based Collaborative Intrusion Detection Networks, in: Cluster Computing, Springer, 2017.

[36] W. Li, W. Meng, L.F. Kwok, Investigating the influence of special on-off attacks on challenge-based collaborative intrusion detection networks, Future Internet 10 (1) (2018) 1–16.

[37] Y. Meng, L.F. Kwok, W. Li, Enhancing false alarm reduction using voted ensemble selection in intrusion detection, Int. J. Comput. Intell. Syst. 6 (4) (2013) 626–638.

[38] Y. Meng, L.F. Kwok, Adaptive blacklist-based packet filter with a statistic-based approach in network intrusion detection, J. Netw. Comput. Appl. 39 (2014) 83–92.

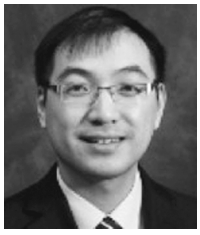
[39] W. Meng, W. Li, L.F. Kwok, Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection, Secur. Commun. Netw. 8 (18) (2015) 3883–3895.

[40] W. Meng, W. Li, L.F. Kwok, EFM: enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism, Comput. Secur. 43 (2014) 189–204.
[41] W. Meng, E.W. Tischhauser, Q. Wang, Y. Wang, J. Han, When intrusion detection meets blockchain technology: A review, IEEE Access 6 (1) (2018) 10179–10188.
[42] Y. Meng, L.F. Kwok, W. Li, Towards designing packet filter with a trust-based approach using bayesian inference in network intrusion detection, in: Proceedings of SecureComm 2012, 2012, pp. 203–221.
[43] Y. Meng, W. Li, L.F. Kwok, Evaluation of detecting malicious nodes using bayesian model in wireless intrusion detection, in: Proceedingsof NSS, 2013, pp. 40–53.
[44] E. Ozdalga, A . Ozdalga, N. Ahuja, The smartphone in medicine: a review of current and potential use among physicians and students, J. Med. Internet Res. 14 (5) (2012) e128.
[45] X. Ruan, Z. Wu, H. Wang, S. Jajodia, Profiling online social behaviors for compromised account detection, IEEE Trans. Inf. Forensics Secur. 11 (1) (2016) 176–187.
[46] W. Meng, M.N. Au, Towards Statistical Trust Computation for Medical Smartphone Networks Based on Behavioral Profiling, in: Proceedings of the 11th IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2017), June, 2017. pp. 152–159.

Weizhi Meng is currently an assistant professor in the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Kongens Lyngby, Denmark. He obtained his Ph.D. degree in Computer Science from the City University of Hong Kong (CityU), Hong Kong in 2013. He won the Outstanding Academic Performance Award during his doctoral study, and is a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in both 2014 and 2017. He was known as Yuxin Meng and prior to joining DTU, he worked as a research scientist in Infocomm Security (ICS) Department, Institute for Infocomm Research, Singapore. He is a member of ACM and IEEE. His primary research interests include intrusion detection, mobile security, biometric authentication, HCI security, cloud security, trust computation, and CPS/IoT security.

Wenjuan Li is currently a Ph.D. student in the Department of Computer Science, City University of Hong Kong (CityU). Prior to this, she worked as a Research Assistant in CityU from 2013 to 2014, and was previously a Lecturer in the Department of Computer Science, Zhaoqing Foreign Language College, China. She was a Winner of Cyber Quiz and Computer Security Competition, Final Round of Kaspersky Lab "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. She is a student member of IEEE.

Yu Wang received his Ph.D. degree in computer science from Deakin University, Victoria, Australia. He is currently an associate professor with the School of Computer Science, Guangzhou University, China. His research interests include network traffic analysis, mobile networks, social networks, and cyber security.



Man Ho Au received his bachelor's and master's degrees from the Department of Information Engineering, Chinese University of Hong Kong, in 2003 and 2005 respectively, and the Ph.D. degree from the University of Wollongong, Australia, in 2009. Currently, he is an assistant professor at Department of Computing, the Hong Kong Polytechnic University. His research interests include public key cryptography, cloud security, information security and privacy. He has published over 90 papers in these areas, including two papers in the ACM CCS Conference that received Runners-Up for the 2009 Pet Award for Outstanding Research in Privacy Enhancing Technologies. He has served as a program committee member for over 30 international conferences.

Please cite this article in press as: W. Meng, et al., Detecting insider attacks in medical cyber–physical networks based on behavioral profiling, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.06.007.