# Towards Statistical Trust Computation for Medical Smartphone Networks Based on Behavioral Profiling

Weizhi Meng[1](✉) and Man Ho Au[2]

[1] Department of Applied Mathematics and Computer Science,
Technical University of Denmark, Kongens Lyngby, Denmark
weme@dtu.dk

[2] Department of Computing, The Hong Kong Polytechnic University,
Hong Kong, Hong Kong
csallen@comp.polyu.edu.hk

**Abstract.** Due to the popularity of mobile devices, medical smartphone networks (MSNs) have been evolved, which become an emerging network architecture in healthcare domain to improve the quality of service. There is no debate among security experts that the security of Internet-enabled medical devices is woefully inadequate. Although MSNs are mostly internally used, they still can leak sensitive information under insider attacks. In this case, there is a need to evaluate a node's trustworthiness in MSNs based on the network characteristics. In this paper, we focus on MSNs and propose a statistical trust-based intrusion detection mechanism to detect malicious nodes in terms of behavioral profiling (e.g., camera usage, visited websites, etc.). Experimental results indicate that our proposed mechanism is feasible and promising in detecting malicious nodes under medical environments.

**Keywords:** Emerging network · Medical smartphone network · Intrusion detection · Insider attack · Statistical trust computation

## 1 Introduction

Over the past decade, healthcare has undergone a significant change through digitizing every aspect of medical infrastructure, including patient records, medical devices and patient/physician communication. As medical industry is evolving rapidly, mobile devices have become a popular platform to carry information and speed up electronic data transfers. For instance, smartphones have been applied in various healthcare organizations, helping record patient's medical conditions and access patient's records in real-time during ward visits. Due to the popularity of smartphones, an emerging medical network has been evolved, called *medical*

W. Meng—The author is previously known as Yuxin Meng.

J.-P. Steghöfer and B. Esfandiari (Eds.): IFIPTM 2017, IFIP AICT 505, pp. 152–159, 2017.
DOI: 10.1007/978-3-319-59171-1_12

*smartphone network (MSN)*, which can be considered as a special kind of wireless sensor network [15]. These devices are generally connected to the organization's wireless network and each of them can be considered as a node. It is known that healthcare organizations (and networked medical devices) are particularly vulnerable to accidental failures, privacy violations, intentional disruption, and widespread disruption [4]. Therefore, there is a great need for protecting MSNs against various attacks, especially insider threats.

Due to the importance and sensitivity of MSNs, it is crucial to identify malicious devices within such network in a fast way. In this work, we advocate the effectiveness of trust-based IDSs and propose a statistical trust-based intrusion detection mechanism to identify malicious nodes in MSNs. In particular, our mechanism employs a statistical trust computation based on behavioral profiling. The contributions of our work can be summarized as below:

- Behavioral profiling is used by IDSs to model system or network events. In this work, we target on behavioral profiling and show how to build a behavioral profile in MSNs.
- As a study, we select four features (e.g., camera usage, visited websites) in building behavioral profiles. Accordingly, we develop a statistical trust computation method to evaluate a node's trustworthiness. Experimental results show that our approach is feasible and promising at identifying malicious MSN nodes in a quick manner.

The remaining parts of this paper are organized as follows. In Sect. 2, we introduce related studies on trust-based intrusion detection mechanisms. Section 3 describes our proposed intrusion detection mechanism and statistical trust computation with selected features. Section 4 describes and analyzes our evaluation, and Sect. 5 concludes our paper.

## 2 Related Work

Insider attacks are one of the major threats for distributed network systems like wireless sensor networks (WSNs). The basic question is how to properly evaluate the trustworthiness of a node.

**Distributed trust-based intrusion detection.** Collaborative intrusion detection networks (CIDNs) [16] have been proposed and implemented, which enable an IDS node to achieve more accurate detection by collecting and communicating information with other IDS nodes.

For instance, Li *et al.* [5] identified that most distributed intrusion detection systems (shortly DIDS) might rely on centralized fusion, or distributed fusion with unscalable communication mechanisms. They then proposed a distributed system according to the emerging decentralized location and routing infrastructure. They assumed that all peers are trusted, which makes the system vulnerable to insider attacks (i.e., betrayal attacks where some nodes suddenly become malicious). To detect insider attacks, Duma *et al.* [1] proposed a P2P-based overlay for intrusion detection (Overlay IDS) that mitigated the insider threat by using a trust-aware engine for correlating alerts and an adaptive scheme for managing trust.

**Challenge-based intrusion detection.** Later, challenge-based CIDNs were proposed, where the trustworthiness of a node depends on the received answers to the challenges. Fung *et al.* [2] proposed a HIDS collaboration framework that enables each HIDS to evaluate the trustworthiness of others based on its own experience by means of a forgetting factor. The forgetting factor can give more emphasis on the recent experience of the peer. Then, they improved their trust management model by using a Dirichlet-based model to measure the level of trustworthiness among IDS nodes according to their mutual experience [3]. This model had strong scalability properties and was robust against common insider threats. Experimental results demonstrated that the new model could improve robustness and efficiency.

To improve the performance, Li *et al.* [6] pointed out that different IDSs may have different levels of sensitivity in detecting particular types of intrusions based on their own signatures and settings. They therefore defined a notion of *intrusion sensitivity* and explored the feasibility of using this notion to evaluate the trust of an IDS node. They further designed a trust management model based on *intrusion sensitivity* to improve the robustness of CIDNs [7], and proposed a machine learning-based approach in automatically allocating the values of *intrusion sensitivity* [8]. Other related studies on improving IDSs can be referred to alert reduction [9], alert verification [13,14] and filtration [10–12].

## 3 Our Approach

According to the recent study [15], 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 security mechanisms can help reduce the number of potential attack vectors. Therefore, a hierarchical trust-based intrusion detection mechanism is one of the potential solutions, which can secure MSNs against insider attacks.

As medical networks are more special than traditional networks, healthcare organizations can define many strict rules and sensitive keywords to control the environment, so the network traffic could be relatively stable in most cases. Due to this, we believe that statistical approach can be used, which may be simple but efficient. Motivated by this, we propose a statistical trust-based intrusion detection mechanism to identify malicious nodes in MSNs.

The high-level detection flows are depicted in Fig. 1, including *behavioral data collection*, *profile construction*, *statistical trust computation*, and *detection and alert*. To collect behavioral data is a crucial step for establishing a robust trust-based intrusion detection scheme. The data are used to build a behavioral profile (as *normal behavior*). Then, the trustworthiness of a node can be computed by our statistical approach through identifying the deviations between the historical profile and current profile. Finally, an alert can be sent to security officers if any trust value is lower than a pre-defined threshold.

**Behavioral Profiling in MSNs.** As described earlier, a behavioral profile is a collection of required information aiming to describe the characteristics of an object under pre-defined rules. For instance, it is similar to a business card that contains some basic features like name, department and business phone number. To create a stable profile, there is a need for using sensible specifications to define the behavior.

Table 1 gives a list of basic features of smartphone users, such as phone calls (including outgoing, incoming and video), location, time, SMS, visited websites, Email address, application usage, etc. It is worth noting that this list provides some common features, but not a full list of those basic features. In MSNs, it is not possible to collect all these data due to its uniqueness and requirements (i.e., there is a chance of leaking information to third-parties). As a study, after communicating and seeking the suggestions from healthcare managers, we choose to collect four features in *each day* to construct a behavioral profile: camera usage, visited websites, Short Message Service (SMS) and Email address. All these features have the potential to be utilized to leak sensitive information, if a device is compromised by attackers.

**Statistical Trust Computation.** In MSNs, security policies usually define 'good' behavior; thus, it is not hard to detect anomalies. However, as network communication is dynamic and hard to predict, it can greatly increase false positives if identifying a malicious node via only one or two unusual events. As a result, trust values can be used to evaluate the severity of unusual behavior. As a study, our work proposes a statistical approach for computing a node's trust value. The calculation of trust values ($T$) can be described as below:

**Table 1.** Basic features of smartphone users.

| | | |
|---|---|---|
| Outgoing calls | Incoming calls | Video calls |
| Location | Time | Short Message Service (SMS) |
| Favourite websites | Email address | IP of access points |
| Bluetooth ID | Camera usage | Application usage |
| Keystroke | Downloaded files | Media player usage |

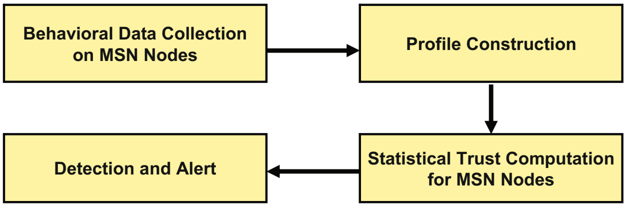
Behavioral Data Collection on MSN Nodes
Profile Construction
Statistical Trust Computation for MSN Nodes
Detection and Alert

**Fig. 1.** The high-level typical detection flows.

$$T = 1 - \prod_{k=1}^{k=n} \frac{M}{I} \quad (n, M, I \in \mathbf{N}) \tag{1}$$

where $n$ denotes the number of features, $M$ represents the number of malicious activities, and $I$ represents the total number of recorded events. Taking two features $A$ and $B$ as an example, if there are two out of ten events and one out of eight events are malicious for $A$ and $B$ respectively, then the trust value is 0.975 $(1 - 2/10 * 1/8)$. Based on Eq. (1), a malicious node can be determined by setting a trust threshold. Let $\tau$ denote the trust threshold, then we can consider:

- If $T \geq \tau$, then the node is considered as a normal node.
- If $T < \tau$, then the node is regarded as a malicious (or untrusted) node.

According to the features of MSNs, our hierarchical trust-based intrusion detection mechanism has two major advantages. *(1) Simple but efficient.* According to Eq. (1), the calculation of trust values is easy through recording required information and data. In addition, the existing central server can mostly have enough computational power and storage space in our scenario. *(2) Fault Tolerance.* As smartphone usage is dynamic, it may produce many false positives by detecting malicious nodes via only one or two unusual events. Thus, our approach considers a set of features in computing trust values, aiming to provide good fault tolerance in practical applications.

# 4 Evaluation

In this section, we evaluate our approach in a healthcare environment located in China. Due to privacy concerns, our mechanism was deployed in a partial MSN, which consists of 10 nodes. A central server was used to collect relevant information from each node and compute trust values, which was composed of an Intel(R) Core (TM)2, Quad CPU 2.66 GHz. In particular, we conduct two major experiments. (1) The first experiment evaluates our mechanism in a normal MSN environment, aiming to observe the trend of trust values and identify a proper threshold. (2) The second experiment explores the feasibility of our mechanism under an adversary scenario, where we randomly select some nodes to behave maliciously (i.e., violating normal profile).

## 4.1 Experiment-1

In this experiment, we attempt to observe the trend of trust values in a normal MSN environment. According to Eq. (1), it is easily understandable if $M$ becomes smaller, then $T$ will become larger. As $M$ is always smaller than $I$, $T$ should fall into the range of [0,1]. A larger $T$ means that a node is more credible. Ideally, $T$ is expected to 1; however, it is very hard to achieve this in real scenarios. Therefore, a major goal of this experiment is to identify a proper threshold for detecting malicious nodes in MSNs. The trend of average and the lowest trust value within a month is depicted in Fig. 2. The main observations are described as follows.

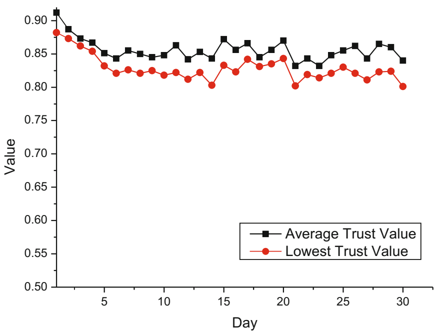

**Fig. 2.** The trend of average and the lowest trust value.

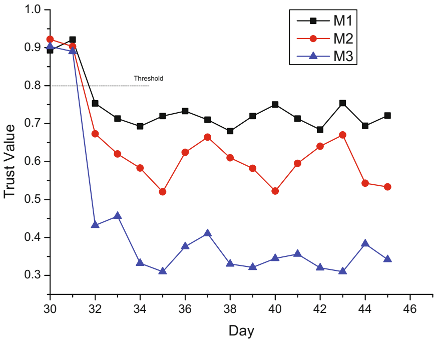

**Fig. 3.** The trust values of malicious nodes in the MSN.

- Average trust value is an average value of all nodes' trust values, which reflects the overall network performance. Figure 2 shows that the trend of average trust value was higher than 0.85 for the first five days. This because the MSN was just initialized and each node required a period of time in connecting with other nodes. Afterwards, average trust value became more stable ranged from 0.84 to 0.87.
- The MSN has 10 nodes, so that the lowest trust value indicates the worst node's performance. Similarly, Fig. 2 describes that the trend of the lowest trust value was peak during the first five days, but gradually decreased and became stable later, ranged from 0.8 to 0.85.

On the whole, it is observed that trust values can be always higher than 0.8 in a normal MSN environment. We believe that the collected one month' data can represent a common MSN performance. Therefore, we choose 0.8 as the trust threshold in this work.

### 4.2 Experiment-2

In this experiment, we aim to evaluate the performance of our approach in a malicious scenario, where some nodes act unusually, i.e., violating the defined profile. More specifically, we randomly selected three nodes (named *M1*, *M2* and *M3*) as malicious to launch unusual events. For example, one node may visit unusual websites in a random way, or send an email to an undefined receiver. The unusual events for each malicious node are summarized in Table 2, where each node could make different unusual events. The malicious actions started from Day 31, and the trust values of these malicious nodes are depicted in Fig. 3. The main observations are described as below.

- As introduced, all three nodes started conducting unusual behavior from Day 31, it is observed that their trust values could quickly decrease to below the threshold of 0.8 at the same day. The trust value of *M1*, *M2* and *M3* ranged from 0.7 to 0.8, from 0.5 to 0.7, and from 0.3 to 0.45, respectively.

**Table 2.** Simulated unusual events for each malicious node.

| Node | Camera usage | Visited websites | SMS | Email address |
|---|---|---|---|---|
| *M1* | √ | - | - | - |
| *M2* | - | √ | √ | - |
| *M3* | √ | √ | - | √ |

- As shown in Table 2, *M1* only violated the usage of camera, while *M3* performed unusual events in relation to camera usage, visited websites and Email address. As a result, *M3* got the lowest trust value among the three malicious nodes.

Overall, the experimental results indicate that threshold of 0.8 is appropriate in our settings, and our mechanism is feasible and promising to identify malicious nodes in a quick manner (i.e., identifying malicious nodes at the same day). Generally, more unusual events result in a lower trust value. This conclusion is also confirmed by IT administrators in the participating healthcare organization.

## 5 Conclusion

With more devices interconnected, medical smartphone networks (MSNs) have become an emerging architecture in healthcare organizations. In this work, we focus on MSNs and propose a statistical trust-based intrusion detection mechanism by combining behavioral profiling and statistical trust computation to detect anomalies. A hierarchical infrastructure is adopted to help control trust computation and apply security policies in MSNs. Experimental results indicate that our proposed mechanism is feasible and encouraging in detecting malicious nodes in a quick manner. This is an early study on designing appropriate trust-based intrusion detection schemes for medical networks. There are many possible topics for our future work. One is to investigate how to efficiently identify a trust threshold in different network environments. It is also an interesting topic to consider more features in trust computation, exploring the impact of each feature and developing a weighted statistical trust computation.

**Acknowledgments.** We would like to thank the cooperation from the participating healthcare managers and IT administrators. Part of this work was supported by the National Natural Science Foundation of China (Grant No. 61602396).

## References

1. Duma, C., Karresand, M., Shahmehri, N., Caronni, G.: A trust-aware, P2P-based overlay for intrusion detection. In: DEXA Workshop, pp. 692–697 (2006)
2. Fung, C.J., Baysal, O., Zhang, J., Aib, I., Boutaba, R.: Trust management for host-based collaborative intrusion detection. In: De Turck, F., Kellerer, W., Kormentzas, G. (eds.) DSOM 2008. LNCS, vol. 5273, pp. 109–122. Springer, Heidelberg (2008). doi:10.1007/978-3-540-87353-2_9

3. Fung, C.J., Zhang, J., Aib, I., Boutaba, R.: 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), pp. 33–40 (2009)
4. Healey, J., Pollard, N., Woods, B.: The Healthcare Internet of Things: Rewards and Risks, March 2015. http://www.mcafee.com/mx/resources/reports/rp-healthcare-iot-rewards-risks.pdf
5. Li, Z., Chen, Y., Beach, A.: 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), pp. 115–122 (2006)
6. Li, W., Meng, Y., Kwok, L.-F.: 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), pp. 518–522. IEEE (2013)
7. Li, W., Meng, W., Kwok, L.-F.: Design of intrusion sensitivity-based trust management model for collaborative intrusion detection networks. In: Zhou, J., Gal-Oz, N., Zhang, J., Gudes, E. (eds.) IFIPTM 2014. IFIP AICT, vol. 430, pp. 61–76. Springer, Heidelberg (2014). doi:10.1007/978-3-662-43813-8_5
8. Li, W., Meng, Y., Kwok, L.-F., Ip, H.H.S.: Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. J. Netw. Comput. Appl. **77**, 135–145 (2017)
9. Meng, Y., Kwok, L.-F.: Enhancing false alarm reduction using voted ensemble selection in intrusion detection. Int. J. Comput. Intell. Syst. **6**(4), 626–638 (2013)
10. Meng, Y., Kwok, L.-F., Li, W.: Towards designing packet filter with a trust-based approach using Bayesian inference in network intrusion detection. In: Keromytis, A.D., Pietro, R. (eds.) SecureComm 2012. LNICST, vol. 106, pp. 203–221. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36883-7_13
11. Meng, Y., Li, W., Kwok, L.: Evaluation of detecting malicious nodes using Bayesian model in wireless intrusion detection. In: Lopez, J., Huang, X., Sandhu, R. (eds.) NSS 2013. LNCS, vol. 7873, pp. 40–53. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38631-2_4
12. Meng, W., Li, W., Kwok, L.-F.: EFM: enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism. Comput. Secur. **43**, 189–204 (2014)
13. Meng, Y., Kwok, L.-F.: Adaptive blacklist-based packet filter with a statistic-based approach in network intrusion detection. J. Netw. Comput. Appl. **39**, 83–92 (2014)
14. Meng, W., Li, W., Kwok, L.-F.: Design of Intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection. Secur. Commun. Netw. **8**(18), 3883–3895 (2015)
15. Meng, W., Li, W., Xiang, Y., Choo, K.-K.R.: A Bayesian Inference-based detection mechanism to defend medical smartphone networks against insider attacks. J. Netw. Comput. Appl. **78**, 162–169 (2017)
16. Wu, Y.-S., Foo, B., Mei, Y., Bagchi, S.: Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS. In: Proceedings of the 2003 Annual Computer Security Applications Conference (ACSAC), pp. 234–244 (2003)