Enhancing collaborative intrusion detection networks using intrusion sensitivity in detecting pollution attacks

Wenjuan Li
Department of Computer Science, City University of Hong Kong, Hong Kong, Hong Kong, and
Weizhi Meng
Department of Computer Science, City University of Hong Kong, Hong Kong, Hong Kong, and Infocomm Security Department, Institute for Infocomm Research, Singapore

Received 6 December 2014
Revised 6 February 2015
10 March 2015
Accepted 11 March 2015

Abstract

Purpose – This paper aims to propose and evaluate an intrusion sensitivity (IS)-based approach regarding the detection of pollution attacks in collaborative intrusion detection networks (CIDNs) based on the observation that each intrusion detection system may have different levels of sensitivity in detecting specific types of intrusions.

Design/methodology/approach – In this work, the authors first introduce their adopted CIDN framework and a newly designed aggregation component, which aims to collect feedback, aggregate alarms and identify important alarms. The authors then describe the details of trust computation and alarm aggregation.

Findings – The evaluation on the simulated pollution attacks indicates that the proposed approach is more effective in detecting malicious nodes and reducing the negative impact on alarm aggregation as compared to similar approaches.

Research limitations/implications – More efforts can be made in improving the mapping of the satisfaction level, enhancing the allocation, evaluation and update of IS and evaluating the trust models in a large-scale network.

Practical implications – This work investigates the effect of the proposed IS-based approach in defending against pollution attacks. The results would be of interest for security specialists in deciding whether to implement such a mechanism for enhancing CIDNs.

Originality/value – The experimental results demonstrate that the proposed approach is more effective in decreasing the trust values of malicious nodes and reducing the impact of pollution attacks on the accuracy of alarm aggregation as compare to similar approaches.

Keywords CIDN, Intrusion detection, Trust computation

Paper type Research paper

1. Introduction

Network intrusions such as virus, Trojan, denial-of-service (DoS) attacks are a challenging threat for computer and network security. For example, intrusion behaviours may cause a great damage of systems, even financial loss. To address this issue, intrusion detection systems (IDSs) have been widely implemented in various

Information & Computer Security
Vol. 24 No. 3, 2016
pp. 265-276

2056-4961
DOI 10.1108/ICS-12-2014-0077

environments aiming to defend against such attacks, and these detection systems have already become an essential component for current network security infrastructure (Scarfone and Mell, 2007).

Generally, there are two types of IDSs: signature-based IDS and anomaly-based IDS. A signature-based IDS (or misuse detection) (Roesch, 1999) detects an attack by comparing its stored signatures with incoming payloads, whereas an anomaly-based IDS (Ghosh *et al.*, 1998) identifies an anomaly by detecting significant deviations between normal profiles and incoming events. In addition, hybrid detection (Hwang *et al.*, 2007) has also been developed that combines the merits from both signature-based detection and anomaly-based detection.

Nowadays, intrusions have become more and more sophisticated and harmful with the rapid development of networks; a single IDS usually cannot identify some complex attacks such as DoS attacks (Symantec Corp., 2012). To solve this problem, IDS collaboration is widely adopted as an effective way to improve the detection capability of a single IDS (or an IDS node). Thus, collaborative intrusion detection networks (CIDNs) (Wu *et al.*, 2003) have been developed with the purpose of enhancing a single IDS in identifying novel or complex attacks through collecting knowledge and learning experience from other IDS nodes.

However, attackers can still compromise some IDS nodes within a CIDN and utilize these compromised nodes to invade the collaborative network. For example, these malicious peers can launch several attacks such as Sybil attacks and pollution attacks to decrease the effectiveness of a CIDN by sending out false information and to compromise other honest IDS nodes. Therefore, designing a robust CIDN and trust computation becomes a crucial topic to improve the detection capability and protect this kind of collaborative networks from insider attacks.

In our previous work (Li *et al.*, 2013), we identified that various IDS nodes may have different levels of sensitivity in detecting particular types of intrusions based on their own signatures and settings. For example, if a signature-based IDS node has more numbers of signatures (or rules) in detecting DoS attacks, then it should be considered as more powerful in detecting such attacks than other nodes (which have relatively fewer related signatures). This observation is very helpful when making decisions in terms of the collected information from different nodes. In this case, we propose a notion of intrusion sensitivity (IS) to emphasise the impact of expert nodes in identifying attacks and ranking alerts. The definition of intrusion sensitivity is:

-IS describes different levels of detection capability (or accuracy) for distinct IDS nodes in detecting particular attacks or anomalies.

1.1 Contributions

In our previous study, we did not consider pollution attacks. In this paper, based on our previous work (Li *et al.*, 2013), we further describe how to apply IS for aggregating alarms and exploring its effect on defending against pollution attacks in which a group of malicious peers cooperate together by providing false alert rankings. More specifically, the goal of applying IS in this paper is to efficiently decrease the trust values of malicious nodes and reduce the impact of pollution attack on the accuracy of alarm aggregation. The contributions of this work can be summarized as below:

- We begin by introducing the adopted CIDN framework with the details of major components and describing a newly designed aggregation component, which

aims to collect feedback, aggregate alarms and identify important alarms from trusted nodes.

- We then detail the trust computation of IDS node and alarm aggregation based on the proposed IS in which only trusted IDS nodes can contribute to the alarm aggregation.
- We later simulate pollution attacks under the CIDN framework and explore the effect of IS on computing trust values regarding the detection of malicious nodes under these attacks. Moreover, we compare the results with similar approaches in the literature.

The remaining parts of this paper are organized as follows. Section 2 describes our adopted CIDN framework and details major components. Section 3 illustrates how to compute trust values of each node and aggregate alarms from trusted nodes. Section 4 presents our evaluation and explores the performance of our approach regarding the detection of malicious nodes under pollution attacks. Then Section 5 discusses some challenges regarding the IS, and Section 6 introduces related work. Finally, Section 7 concludes this work with future directions.

2. Collaborative intrusion detection network framework

In Figure 1, we present the adopted CIDN framework with major components such as certificate authority (CA), trust management component, collaboration component, communication component, aggregation component and query component. Different from our previous work (Li *et al.*, 2013), we develop a new component called aggregation component in the framework that aims to collect feedback and aggregate alarms. The details of each component are described as follows.

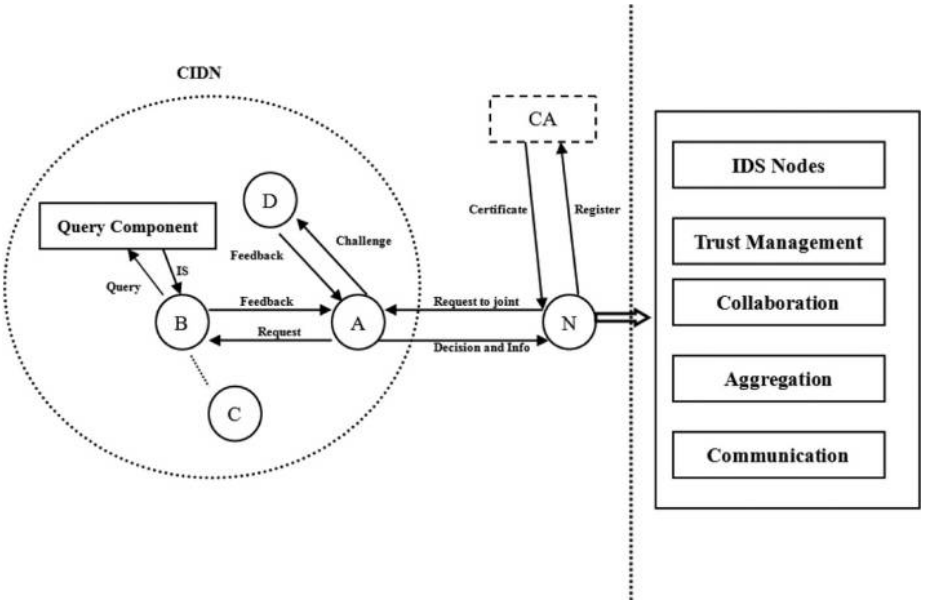

Figure 1. The CIDN framework

2.1 Intrusion detection system nodes

Each node [either a host-based intrusion detection system (HIDS) or a network-based intrusion detection system (NIDS)] can choose its collaborators (or partners) based on its own experience and can maintain a list of their collaborating nodes, which is called a partner list. This list is customizable and contains public keys of other nodes and their trust values.

If a node requests to join this CIDN, it has to register to a trusted CA and obtain its unique proof of identity (including a public key and a private key). For instance, as shown in Figure 1, if a Node *N* wants to join this network, then it can send a request to a Node *A* (or other nodes). After receiving the request, Node *A* can send back its decision (accept or decline). If the decision is acceptance, then Node *N* can join the network and get an initial partner list from Node *A*.

2.2 Query component

Following our previous study (Li *et al.*, 2013), to relax the complexity of assigning IS, a set of IS values will be stored in this component by means of expert knowledge. The use of expert knowledge is useful in deciding the sensitivity levels of different IDS nodes, so in this work, three experts are invited to collaboratively allocate IS values to different nodes.

To obtain the IS values of others, an IDS node can send a query to this component. Then, this component can send feedback with the required values.

2.3 Trust management component

This key component is responsible for evaluating the trustworthiness of other nodes. In a CIDN, an IDS node can compute the trust values of other nodes based on its own information and by learning from other nodes' experience. To obtain the required data in the computation, it can cooperate with other components such as collaboration component through sending and receiving particular messages.

2.4 Collaboration component

This component is mainly responsible for assisting an IDS node to evaluate the trustworthiness of others through sending out some particular messages such as requests, challenges and query messages and collecting the corresponding feedback. These particular messages are described as follows:

- *Requests* can be sent by a node for consulting alert ranking (or other required information). For example, an IDS node can request some target nodes to help determine the ranking of several alerts (or called alarms).
- *Challenges* are sent for evaluating the trustworthiness of other nodes in the partner list. In particular, the node which sends out the challenges knows the desirable answer so that it can evaluate the trustworthiness of other nodes by analysing the received feedback.
- *Query messages* are sent by an IDS node to the query component for requesting IS values for target IDS nodes. The use of IS aims to emphasise the impact of expert nodes in identifying malicious nodes and ranking alarms.
- *Feedback* can be sent back by either IDS nodes or the query component. Generally, if an IDS node receives a request or challenge, it has to send back its feedback as the answer. For the query component, if it receives a query for requesting the IS

values of other nodes, it would send back a list of IS values as the feedback, where this paper specifically denotes such feedback as IS (see Figure 1) aiming to distinguish the feedback responded for a challenge.

2.5 Aggregation component

This is a newly designed component in this work, which is mainly responsible for aggregating alarms by learning the experiences from other trusted IDS nodes and identifying important alarms in terms of a defined threshold. For example, if the value of alarm aggregation exceeds the threshold, then this alarm can be regarded as an important alarm and should be paid more attention; otherwise, the alarm can be considered as a non-critical alarm.

2.6 Communication component

This component is used to communicate with other IDS nodes and provide network communication between different IDS nodes within a CIDN. For instance, for a HIDS-based CIDN, this component can establish peer to peer (P2P) during the communications.

3. Trust computation and alarm aggregation

In this section, we mainly introduce the trust computation and alarm aggregation as compared to the work by Fung *et al.* (2008), which established the trust computation according to the similar CIDN framework used in this work.

As mentioned above, IS attempts to evaluate different levels of detection capability for IDS nodes in detecting particular attacks. In this work, we use five levels of IS: very high (0.95), high (0.7), neural (0.5), low (0.3) and very low (0.1). Note that the specific detection levels can be tuned in a real environment (i.e. setting different levels by means of expert knowledge).

3.1 Trust computation and evaluation

To evaluate the trustworthiness of a target node, an IDS node can firstly sent challenges to this target node by means of a random generation process. When receiving the feedback from the target node, the IDS node can decide a score to reflect its satisfaction level based on the feedback.

Similar to Li *et al.* (2013), we can evaluate the trustworthiness of a Node *i* according to a Node *j* as follows:

$$T_i^j = \left(w_s \frac{\Sigma_{k=0}^{n} F_k^{j,i} I_s^j \lambda^{tk}}{\Sigma_{k=0}^{n} \lambda^{tk}} - T_s \right)(1 - x)^d + T_s \tag{1}$$

where I_s^j ($\in (0,1)$) is the IS level of Node j, $F_k^{j,i}$($\in (0,1)$) denotes the score of the received feedback k, n is the total number of feedback, $\lambda$is a forgetting factor which assigns less weight to older feedback to emphasise on the effect of recent feedback and $w_s$is a significant weight depending on the total number of received feedback. If there are only few feedbacks under a certain minimum m, then $w_s = \Sigma_{k=0}^{n} \lambda^{tk}/m$; otherwise, its value is 1, where T_s is the initial trust value for a new comer and d is the percentage of "don't know" answers during a period (e.g. from *t0* to *tn*), which is useful for newly joined

nodes. It is worth noting that if sending out a number of "don't know" answers, the trust values would be gradually decreased according to equation (1).

3.2 Alarm aggregation

By using the collaboration component, each IDS node can also consult alert ranking from those nodes in its partner list. After receiving the feedback, Node j can aggregate the alarm feedback $R_j(a)$, which is the aggregated ranking of alarm a by considering the experience from other trusted nodes, using a weighted majority method as follows:

$$R_j(a) = \frac{\sum_{T \geq r} T_i^j D_i^j R_i(a)}{\sum_{T \geq r} T_i^j D_i^j}, \tag{2}$$

where $R_i(a)$ ($\in (0,1)$) is the feedback ranking of alert a by Node i, r is a defined threshold, in which Node j requests alert ranking to those nodes whose trust values are higher than this threshold, T_i^j ($\in (0,1)$) is the trust value of Node i according to Node j and D_i^j ($\in (0, 1)$) is a measure of hops between the two nodes. In this work, we consider it as the geographical distance, as feedback from nearby nodes should be more relevant than that from distant ones.

4. Evaluation

In our previous work, we did not consider and evaluate our approach under pollution attacks in which a group of malicious nodes cooperate with each other through sending the CIDN with false alarm rankings. In this section, we mainly attempt to evaluate the performance of our approach in detecting malicious nodes, as compared to Fung *et al.* (2008, 2009), under the simulated pollution attacks.

In the evaluation, our settings are similar to those reported by Fung *et al.* (2008, 2009) so that we can compare these approaches. More specifically, the CIDN is randomly distributed in a 5×5 grid region with up to 30 nodes. Some simulation parameters are presented in Table I. In addition, the feedback satisfaction is classified into five levels as follows: very satisfied (1.0), satisfied (0.5), neutral (0.3), unsatisfied (0.1) and very unsatisfied (0). For the query component, we store a list of IS values for all IDS nodes within the CIDN. Note that these values are decided by means of expert knowledge.

4.1 Mapping of satisfaction level

As described above, the feedback satisfaction is classified into five levels. In this work, we develop a simple statistic-based method of mapping the received feedback into these levels.

In particular, we use Snort in the evaluation, whose alarms have three priority levels: low, medium and high. In the evaluation, a challenge contains five alarms which request

Table I. Simulation parameters in the evaluation

Parameter	Value	Description
λ	0.9	Forgetting factor
T_s	0.5	Trust value for new comers
m	10	Lower limit for received feedback
r	0.75	Trust threshold for alarm aggregation

another node to give correct priority. Intuitively, it is a worse situation if a higher priority alarm was given a lower priority. Thus, this node's feedback should be assigned a lower score (denoted by *score[n]*, where *n* is the alarm number). Our statistic-based method uses the following rules:

- *R1.* For each alarm, if a correct classification is given, then the relevant feedback can get 1 point (*score[.]* = 1).
- *R2.* For each alarm, if a lower priority is given, then the relevant feedback can get 0 point (*score[.]* = 0).
- *R3.* For each alarm, if a higher priority is given, then the relevant feedback can get 0.5 point (*score[.]* = 0.5).

According to the rules presented above, the mapping can be evaluated based on the following final score:

$$FS = \frac{\sum_{n=1}^{N} score[n]}{N} (n, N = 1, 2, 3, \ldots), \tag{3}$$

where *n* is the concrete number of an alarm and *N* is the total number of alarms. In Table II, we illustrate the detailed mapping relationship.

For the satisfied level, we require at least three 1 points plus two 0.5 points; for the neutral level, we require at least five 0.5 points; and for the unsatisfied level, we require at least three 0.5 points. The range is, therefore, organised based on these key points. It is found that this statistic-based mapping performs well in our evaluation, whereas developing a more advanced method is one of our future directions.

4.2 Pollution attack

The aim of the evaluation is to explore the performance of our approach in defending against pollution attacks. More specifically, we begin by running the network over a period (e.g. ten days) to make it stable. Then, we launched this attack (i.e. from the 11th day) by randomly selecting three nodes and utilising these nodes to send false alarm rankings.

As IDS nodes can send challenges to others periodically, these malicious nodes under pollution attacks can be identified after a period of time. The evaluation results of detecting malicious nodes and the impact of the accuracy of alarm aggregation are shown in Figures 2 and 3, respectively.

Figure 2 shows that our approach can identify the malicious nodes more quickly than the trust models of Fung *et al.* (2008 and 2009). For instance, using our

Final score (FS)	Satisfaction level	Mapping value
1	Very satisfied	1
(1,0.8)	Satisfied	0.5
(0.8,0.5)	Neutral	0.3
(0.5,0.3)	Unsatisfied	0.1
(0.3,0)	Very unsatisfied	0

Table II. Mapping of satisfaction level

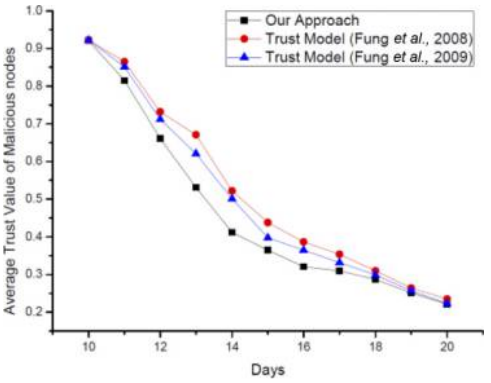

Figure 2.
Trust values of malicious nodes

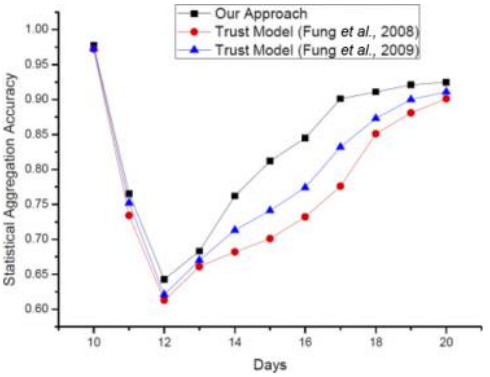

Figure 3.
The impact of pollution attack on alarm aggregation

approach, the average trust value of malicious nodes drops faster to 0.661 on Day 12, whereas the value only drops to 0.732 and 0.712 if using the approach given by Fung *et al.* (2008 and 2009), respectively. These results indicate that our approach is more sensitive and effective in detecting pollution attacks than the other two similar approaches by emphasising the impact of expert nodes (i.e. with higher IS).

In Figure 3, we present the impact of pollution attacks on the accuracy of alarm aggregation. It is visible that our approach can reduce the negative impact on alarm aggregation earlier than those reported by Fung *et al.* (2008) and 2009). For example, our approach can recover the accuracy of alarm aggregation more quickly, as malicious nodes can be detected earlier. When the trust values of these nodes fall below the threshold of 0.75, then these nodes cannot affect the alarm aggregation. These results show that our approach is effective in detecting pollution attacks and mitigate their impact.

In our previous work (Li *et al.*, 2013), we have shown that our approach is effective in detecting malicious nodes under Betray attacks. Overall, the experimental results in this work indicate that our approach, which integrates with IS, is more effective in detecting insider attacks through identifying malicious nodes more quickly as compared to Fung *et al.* (2008, 2009).

5. Further discussions

This work illustrates how to defend against pollution attacks based on the proposed IS. However, there are still several challenges in this area:

- *Evaluation of IS*: In this work, we evaluate the sensitivity of an IDS node by means of expert knowledge; however, this is not an objective way. For instance, different experts might have different views in evaluating the capability of a node based on their own knowledge, so that disagreement may exist to evaluate the detection capability of a node. To mitigate this issue, it is an open challenge to identify and develop an objective method of evaluating the IS of an IDS node.
- *Allocation of IS*: In this paper, the specific values of IS are assigned by a query component based on expert knowledge. However, this method may request huge human efforts in a large-scale network as the number of IDS nodes becomes very large. In this case, it is promising to develop an automatic process to assign the levels of IS. For example, in another work (Li *et al.*, 2014), we used a k-nearest neighbors (KNN) classifier to automatically allocate the values of IS to each node and achieved promising performance. Thus, more efforts can be made to develop more efficient and accurate approaches in allocating these values.
- *Update of IS*: In real-world applications, it is identified that IDS signatures (even heuristic approach) would be updated periodically, so the specific values of IS should be updated accordingly. Our work does not consider this issue at the current stage, but it is a big challenge in our future work to develop additional feedback or control mechanisms to update IS.
- *Mapping of satisfaction level*: In this work, we use a relatively naive statistic-based approach to compute the satisfaction level by mapping nodes' feedback to the challenges. This approach can ease the computational workload, but we notice that a more advanced approach should be used in a complex or dishonest environment. Under those environments, some malicious nodes may attack the specific mapping method, so it is a challenge to design a more robust mapping of the satisfaction level.
- *Collaboration of malicious nodes*: In the evaluation, we simulate simple pollution attacks by sending false alarm rankings. However, in a dishonest environment, the way of collaboration between malicious nodes would be more complicated. It is also a big challenge to evaluate different trust models in a large-scale network.

6. Related work

A lot of trust models have been proposed to identify malicious nodes or peers in CIDNs. For example, Janakiraman and Zhang (2003) focused on the case of distributed IDSs running over P2P networks and proposed Indra, a distributed scheme based on sharing information between trusted peers in a network. It can offer a scalable solution by providing for security plug-ins that can be loaded on the fly simultaneously by thousands of machines in an administrative domain. Then, Li *et al.* (2006) identified that most distributed intrusion detection systems (DIDS) relied on centralized fusion, or distributed fusion with unscalable communication mechanisms, and then proposed a DIDS based on distributed hash table (DHT). In particular, they embedded the intrusion symptoms into the DHT dimensions so that alarms related to the same intrusion could be routed to the same sensor fusion centre with good load balancing. The experimental results showed that their approach could

greatly outperform the traditional hierarchical approaches when facing large amounts of diverse intrusion alerts. However, these approaches assume that all peers are trusted, which can be vulnerable to insider attacks.

To defend against insider attacks, Duma *et al.* (2006) 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. The trust-aware correlation engine is capable of filtering out warnings sent by untrusted or low quality peers, whereas the adaptive trust management scheme uses past experiences of peers to predict their trustworthiness. Several other related work can be referred to Ding *et al.* (2013), Ho *et al.* (2012), Li *et al.* (2012) and Nagaraja *et al.* (2010). But, a major problem is that the past experience of a peer has the same impact regardless of the age of its experience.

To solve this issue, Fung *et al.* (2008) presented a trust-based HIDS collaboration framework which could enhance intrusion detection within a host-based IDN. Their framework 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. Their simulations demonstrated the improved performance of the framework in detecting intrusions and their robustness against malicious attacks. Later, Fung *et al.* (2009) improved their proposed trust management model by adopting the Dirichlet family of probability density functions in the trust management for estimating the likely future behaviour of a HIDS based on its past history. This model had strong scalability properties and was robust against common insider threats. The experimental results demonstrated that the new model could improve robustness and efficiency.

In our previous work, we identify that each IDS node has some special expertise in detecting certain attacks. That is, different IDS nodes may have different levels of sensitivity in detecting different types of intrusions. This is our motivation to define the notion of IS by emphasising the impact of an expert IDS. In this work, we further explore the performance of the IS-based approach in defending against pollution attacks and evaluate its impact on alarm aggregation as compared to Fung *et al.* (2008) and 2009).

7. Conclusion and future work

In this work, we mainly propose and evaluate an IS-based approach to enhance the performance of CIDNs in detecting pollution attacks and aggregating alarms. We identify that different IDS nodes may have distinct capabilities in detecting intrusions. Thus, IS is defined to describe different levels of capability of IDS nodes in detecting particular attacks. More specifically, we first introduce the CIDN framework with major components and then describe the computation of trust values and the aggregation of alarm ranking. In the evaluation, we explore the performance of our approach in detecting pollution attacks and aggregating alarms from other trusted nodes. The experimental results indicate that our approach is more effective in decreasing the trust values of malicious nodes and reducing the impact of pollution attacks on the accuracy of alarm aggregation as compared to similar approaches.

Our work is at an early stage, and there are many possible topics. Future work could include developing other trust types such as recommendation trust to improve the trust computation of IDS nodes. Additionally, future work could also include exploring how to decide IS values more objectively and how to allocate these values more intelligently.

References

Ding, L., Yu, F., Yang, Z. and Yue, G. (2013), "The system design of a node of P2P networks for intrusion detection", *Journal of Networks*, Vol. 8 No. 8, pp. 1920-1927.

Duma, C., Karresand, M., Shahmehri, N. and Caronni, G. (2006), "A trust- aware, P2P-based overlay for intrusion detection", *Proceedings of DEXA Workshop*, *Krakow*, pp. 692-697.

Fung, C.J., Baysal, O., Zhang, J., Aib, I. and Boutaba, R. (2008), "Trust management for host-based collaborative intrusion detection", *Proceedings of DSOM*, *Samos Island*, pp. 109-122.

Fung, C.J., Zhang, J., Aib, I. and Boutaba, R. (2009), "Robust and scalable trust management for collaborative intrusion detection", *Proceedings of the 2009 IFIP/IEEE International Symposium on Integrated Network Management*, *Long Island, NY*, pp. 33-40.

Ghosh, A.K., Wanken, J. and Charron, F. (1998), "Detecting anomalous and unknown intrusions against programs", *Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC)*, *Phoenix, AZ*, pp. 259-267.

Ho, C.Y., Lai, Y.C., Chen, I.W., Wang, F.Y. and Tai, W.H. (2012), "Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems", *IEEE Communications Magazine*, Vol. 50 No. 3, pp. 146-154.

Hwang, K., Cai, M., Chen, Y. and Qin, M. (2007), "Hybrid intrusion detection with weighted signature generation over anomalous internet episodes", *IEEE Transactions on Dependable and Secure Computing*, Vol. 4 No. 1, pp. 41-55.

Janakiraman, R. and Zhang, M. (2003), "Indra: a peer-to-peer approach to network intrusion detection and prevention", *Proceedings of the 12th IEEE International Workshops on Enabling Technologies*, *Washington, DC*, pp. 226-231.

Li, W., Meng, Y. and Kwok, L-F. (2013), "Enhancing trust evaluation using intrusion sensitivity in collaborative intrusion detection networks: feasibility and challenges", *Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS)*, *Leshan*, pp. 518-522.

Li, W., Meng, Y. and Kwok, L.F. (2014), "Design of intrusion sensitivity-based trust management model for collaborative intrusion detection networks", *Proceedings of the 8th IFIP WG 11.11 International Conference on Trust Management (IFIP TM)*, *Singapore*, pp. 61-76.

Li, X., Zhou, F. and Yang, X. (2012), "Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23 No. 10, pp. 1944-1957.

Li, Z., Chen, Y. and Beach, A. (2006), "Towards scalable and robust distributed intrusion alert fusion with good load balancing", *Proceedings of LSAD*, *New York, NY*, pp. 115-122.

Nagaraja, S., Mittal, P., Hong, C.Y., Caesar, M. and Borisov, N. (2010), "Botgrep: finding P2P bots with structured graph analysis", *Proceedings of USENIX Security 2010*, *Berkeley, CA*, pp. 1-16.

Roesch, M. (1999), "Snort: lightweight intrusion detection for networks", *Proceedings of LISA*, Berkeley, CA, pp. 229-238.

Scarfone, K. and Mell, P. (2007), *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST Special Publication, pp. 800-894.

Symantec Corp (2012), "*Internet Security Threat Report*", Vol. 16, available at: www.symantec.com/business/threatreport/index.jsp

Wu, Y.S., Foo, B., Mei, Y. and Bagchi, S. (2003), "Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS", *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC)*, *Washington, DC*, pp. 234-244.

About the authors

Wenjuan Li is currently a PhD student in the Department of Computer Science, City University of Hong Kong. She was previously a research assistant in the CS department of CityU and a Lecturer in the Department of Computer Science, Zhaoqing Foreign Language College, China. Her research interests include network security, intrusion detection, trust computing, web technology and E-commerce Technology. Wenjuan Li is the corresponding author and can be contacted at: wenjuanqiqi@163.com

Weizhi Meng received his BEng degree in Computer Science from the Nanjing University of Posts and Communications in 2009 and PhD degree in Computer Science from the City University of Hong Kong in 2013. He was known as Yuxin Meng and is currently a Research Scientist in Infocomm Security Department, Institute for Infocomm Research, Singapore. Prior to this, he was employed by the CS Department, City University of Hong Kong, as a Senior Research Associate. His research interests are information security including intrusion detection, mobile authentication and security, Web security, malware analysis, cloud computing and intelligent security applications. He is a member of the IEEE and ACM.