International Journal of Engineering & Technology, 7 (4.31) (2018) 352-356

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Super-Peer Approach for Scalable Collaborative Intrusion Detection Network (CIDN)

Yousef Bakhdlaghi[1*], Nur Izura Udzir[2], Azizol Abdullah[3] and Nor Fazlida Mohd Sani[4]

[1]*Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*
[2]*Faculty of Computing and Information Technology, University of Jeddah, 285 Dhahban 23881, Saudi Arabia*
**Corresponding author E-mail: ybakhdlaghi@uj.edu.sa*

Abstract

Collaborative intrusion detection systems (CIDSs) have the ability to correlate suspicious activities from various CIDSs in different networks to maximize the efficiency of the intrusion detection in addition to sharing the knowledge and resources among them. Current consultation-based CIDNs do not honor the scope variations of CIDSs (area of expertise). Evaluating collaborators' knowledge regardless of their scope variations could degrade the efficiency of the CIDN, while in reality CIDSs have different platforms and strengths in various areas that could affect the overall scalability and efficiency of the architecture negatively. Additionally, many architectures in the literature built under information-based settings, while few architectures have the consultation-based capabilities. An architecture that combines both information-based and consultation-based capabilities has not been proposed yet. This paper proposes a scope-aware super-peer collaborative intrusion detection network (CIDN) architecture that takes CIDS scope into consideration when consulting, by organizing CIDSs into groups based on their scope regardless of their physical locations as well as incorporating the information-based into the consultation-based architecture to benefit from consultation-based capabilities while limiting the information being distributed to fast-spreading attacks that are discovered from consultation requests. However, the proposed architecture can strengthen the efficiency of the CIDN as well as reducing the overload of the communications among collaborators and contributes to enhance the overall scalability of the architecture.

Keywords: *Collaborative intrusion detection network; Intrusion detection; Network security; Scalable CIDN; Super-peer architecture.*

1. Introduction

Internet and the networked environments facilitate linking computers and network devices and offer high availability worldwide for services and resources. These devices are subject to defacement, information stealing, and compromise by hackers who find and develop exploits to leverage and get advantage of vulnerabilities in systems and applications. In contrast, researchers and information security personnel are trying hard to discover and countermeasure these attacks and make it much difficult to attack and stay secure by developing systems to detect the presence of attacks or attack attempts. However, intrusion detection systems (IDSs) provides monitoring and inspection capabilities for identifying suspicious activities. Yet, a single IDS may not have the ability to discover new threats but collaborating with other IDSs can extend its capabilities to discover new attacks.

Moreover, collaborative intrusion detection network (CIDN) has the ability to correlate suspicious activities from various collaborative intrusion detection systems (CIDSs) in different networks to maximize the efficiency of the intrusion detection in addition to sharing knowledge and resources among them which allows the IDS to discover large-scale and coordinated attacks. CIDN falls into two types: information-based and consultation-based. In information-based CIDN, collaborators share their knowledge, observation and warn others about intrusions and large-scale attacks. While in consultation-based CIDN, no information or warnings are distributed within the CIDN, instead, it gives the ability for a CIDS to consult other CIDSs when it lacks knowledge and confidence about any suspicious activity [1][2].

Generally, an architecture of a networked system can be categorized into: centralized, decentralized, and hybrid. The centralized architecture is referred to as client-server model where the server offers services for clients providing a centralized control of services in one server which might be beneficial for some applications, but it poses several weaknesses such as: single point of failure, and limited resources. While in the decentralized architecture, there is no centralized server, thus, no single point of failure. Instead, each peer will act as a client (requesting for services) and server (acting to requests). This architecture also has some weaknesses such as: increasing traffic as the network grows especially if it is not structured properly and lacks central management. Peer-to-peer (P2P) network is an example of decentralized architecture. The limitations of both centralized and decentralized architectures can be overcome in the hybrid architecture as in super-peer networks. Super-peer, in P2P networks, is a peer that has the features of normal peer in the decentralized architecture and offers some of the centralized architecture features [3].

However, scalability is an important goal to achieve in distributed systems and there are several dimensions to measure the scalability of distributed systems: the size of which the system can easily accommodate more users and resources, the ability of having users and resources that lie in different geographical locations, and its administration remains manageable. Yet, it is possible to encoun-

ter some performance loss as the system scales up [4]. This scalability issue has introduced super-peer networks in P2P file sharing systems where the super-peer acts like a centralized server to a group of peers maintaining a list of available peers and their shared files, then exchanges this information with other super-peers. Also, it receives queries from its peers and replies them with answers, forming a hierarchy of organized P2P architecture [5]. Thus, using super-peer networks can contribute to reduce traffic overload and management cost in P2P systems [6][15].

Current consultation-based CIDNs used unstructured peer-to-peer architecture that might cause scalability issues as it scales up. Also, the variations of CIDS scopes in the architecture have not been addressed, leaving each IDS with a list of peers to evaluate by its own. However, evaluating collaborators' knowledge regardless of their scope variations could degrade the efficiency of the CIDN, while in reality CIDSs have different strengths in various areas. This could affect the overall scalability of the architecture negatively since it increases the overhead of unnecessary consultation requests to inexpert peers, affecting the decision made by CIDS. Also, obtaining acquaintance list is an issue that has not been addressed previously in CIDN. However, many architectures in the literature [7-15] built under the information-based settings, while few recent architectures have the consultation-based capabilities [2, 16-18], but an architecture that takes scope into consideration when consulting and incorporates both information-based and consultation-based capabilities that also facilitates obtaining acquaintance list has not been proposed yet.

Notwithstanding the above limitations, this paper proposes a scalable collaborative intrusion detection network (CIDN) architecture that takes IDS scopes into consideration when consulting besides incorporating consultation-based and information-based capabilities in one architecture by introducing the concept of super-peer to achieve that. The proposed architecture can strengthen the efficiency of the CIDN by reducing the chances of consulting inexpert peers that affects the decision CIDS makes. It also enhances the scalability and the ability to accommodate more peers, without losing the control of the CIDN or creating a single point of failure, which facilitates obtaining acquaintance list to enhance the overall scalability of the architecture. The super-peer employment in the architecture can limit the information being distributed to fast-spreading attacks or the severe ones that discovered from consultation requests within the CIDN.

The rest of this paper organized as follows: (2) a review of current and related CIDN architectures, (3) the proposed CIDN architecture, (4) scalability analysis and evaluation, (5) conclusion and future work.

2. Related Work

Collaborative intrusion detection network (CIDN) has the ability to discover large-scale and coordinated attacks. It falls into two types: information-based, and consultation-based. The majority of existing CIDNs are built on information-based settings; alerting other peers when an IDS detects a suspicious activity or gathering these alerts from one or more locations to correlate and get the global view of possible threats [7-15]. Some of these architectures employed a trust mechanism among collaborators [9, 11, 15], while others assumed that collaborators are trusted [7, 10, 13, 14], or their warnings or alerts will not be distributed unless verified by a parent node in a hierarchy architecture [12, 15].

On the other hand, a few papers discussed the consultation-based CIDN that limits the communications between collaborators to consultation only when a CIDS lacks the knowledge about a suspicious activity [2, 16-18]. However, the trust evaluation was an important component in their CIDN design that minimizes the impact of insider attacks (malicious peers). Although the network structure used in their papers is pure P2P with consultation-based settings, the negative impact on scalability is less compared to the information-based architectures since the collaboration is on-demand unlike the information-based that shares their alerts and warning to others. But, still there is a chance to encounter some scalability issues as the CIDN scales up even in consultation-based CIDN. Nevertheless, using super-peer networks can contribute to reduce traffic overload and management cost in P2P systems [6][15].

From the previous works on CIDN, we can conclude that scalability can be viewed from two different aspects; the scalability of the architecture itself, and the scalability of the consultation and decision process on each CIDS. The first aspect reflects the ability of the architecture to accommodate additional users to the CIDN in structured manner that reduces the negative impact on the overall performance of CIDN, while the second one is concerned about the ability to have a reliable result by each CIDS as the CIDN scales up.

To the best of our knowledge, an architecture that gets the benefit of both information-based and consultation-based capabilities to limit the information being distributed to fast-spreading attacks has yet to be proposed. Although the super-peer concept was previously introduced [15] to cluster the CIDSs into groups based on their closeness, it does not allow a CIDS within a group to share the knowledge with other groups since it was built on the information-based architecture. Whereas in this work, the groups are based on their scope and the consultation-based capability allows each peer within a group to consult other groups' members based on the area of that suspicious activity.

3. The Proposed Architecture

This section discusses the proposed architecture that adopts the super-peer network architecture into the CIDN to get the benefits of both centralized and decentralized architectures, plus having the capabilities of information-based and consultation-based CIDN in one architecture. The proposed architecture consists of two types of collaborators: peer and super-peer. The super-peer offers some centralized architecture features, while peers are grouped by their area of expertise (scope) - regardless of their physical locations - with at least one peer on each group designated as a super-peer that is operated and managed by human expert which could be a security firm or organization. It is also possible to have more than one super-peer for one group as the CIDN scales up. The number of groups is known for all collaborators within the CIDN, and all of them will be notified if there is a change. Collaborators that are expert in a particular scope will be grouped together and a new collaborator with similar expertise will join the same group. So, any consultation request in that area of expertise will be sent to the members of that group. Each super-peer maintains information about that group and this information is exchanged and updated between super-peers.

However, the information-based employment in the proposed architecture is achieved through super-peers by detecting recent consultation requests for the same suspicious activities or attacks that take place in the CIDN to be distributed to other collaborators within the same group. This way, collaborators will be updated with information on the detected fast-spreading attacks within their scope. So, before a collaborator request a consultation, it queries its knowledge that is received from super-peer updates, and if it finds the desired information, no consultation request will be made. This reduces the overhead of consultation requests rate between peers' resources consumption and contributes to alert the group peers about latest fast-spreading attacks in addition to bringing their attention to overlooked attacks that is taking place recently in this group.

Furthermore, dividing collaborators into groups based on their scope plus employing the super-peer collaboration concept can contribute to enhance the scalability and the ability to accommodate more peers, without losing the control of the CIDN or creating a single point of failure. Besides, this will also help in strengthening the efficiency of the CIDN by reducing the chances

of consulting inexpert peers and thus, affecting the decision that is made by a CIDS.

Fig. 1 shows the topology of the proposed architecture which allows peers to be organized into several groups according to their scope. All consultation requests will be sent to the relevant group that is specialized in this type of attacks. So, each peer within a group can consult peers that are in its group or other groups depending on the scope of consultation request. Each group must have at least one super-peer and it should be included in every consultation request a peer makes. It is possible to have multiple super-peers for a group as the CIDN grows up. The information about peers from different groups are exchanged and updated by super-peers.

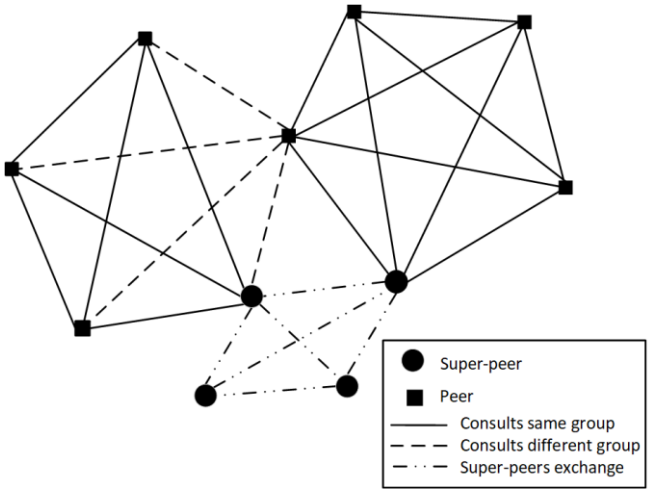

Fig. 1: Topology View of the Proposed Architecture

3.1. Architecture Components

As illustrated in Fig. 2, the proposed architecture consists of several components: Consultation Unit, Trust and Evaluation Unit, Acquaintance Management Unit, and Decision Unit in addition to super-peers' updates and communication among peers and super-peers.

3.1.1. Consultation Unit

The Consultation Unit maintains the information received from the super-peer about fast-spreading attacks updates within the CIDN. Whenever a CIDS wants to consult the group regarding a certain suspicious activity, it checks the updates received from the group's super-peer first, to see whether or not this suspicious activity has been previously detected in the CIDN. If it is not available from its super-peer, the Consultation Unit initiates a consultation request that goes to the Trust and Evaluation component to proceed with the request.

3.1.2. Trust and Evaluation Unit

This unit gives the ability to evaluate the trustworthiness of peers based on past experiences, either from previous real consultation requests or test ones. This helps in maintaining acquaintance list by updating the trustworthiness of peers in the list and remove the incompetent ones. The probation list keeps track of the removed peers from the acquaintance list. Each peer in this list is evaluated with test consultation requests only (not real consultation requests). The top evaluated peers in the probation list will be considered to be added back into the acquaintance list if needed.

Once a peer received a request from the Consultation Unit, it sends the consultation request to peers (including super-peer) in the group that this suspicious activity belongs. The trustworthiness of peers is taken into consideration when requesting for consultations and when performing feedback aggregation.

3.1.3. Acquaintance Management Unit

This unit maintains a list of peers for each group of expertise. An initial list of peers is received from the super-peer when joining a group in the CIDN. This list gets regular updates from super-peer as new peers joined or removed. Each peer will have its own acquaintance list that is selected from available peers. Maintaining the acquaintance list is achieved based on feedbacks to real or test consultation requests. Whenever a peer's trustworthiness drops to a certain level, it will be moved to the probation list for further evaluation with test consultation requests only.

3.1.4. Decision Unit

The Decision Unit is responsible for aggregating the received feedbacks from other peers. The trustworthiness of each peer is taken into consideration during feedbacks aggregation. The Decision Unit works with the Trust and Evaluation Unit in assessing the satisfaction of received feedbacks and also getting the trustworthiness value of peers for aggregation process. There will be no aggregation. the other hand, if the peer has the knowledge about a suspicious activity (from the updates or its own knowledge).

3.1.5. Super-Peer Updates

Super-peer sends updates to its group's peers about discovered fast-spreading attacks, and when new peers joined or are removed from the CIDN. The information of the groups is exchanged and updated between super-peers (within the same group or different groups), including initial acquaintance list of each group in addition to new available peers.

3.1.6. Peers/Super-Peers Communication

All communications and interactions with other peers and super-peers are handled by this component. A public key infrastructure (PKI) can be used in the CIDN architecture to secure communication between peers and to prove identity. Each peer has its own public key that is known to other peers and super-peers too. This also helps in preventing man-in-the-middle (MITM) attack.

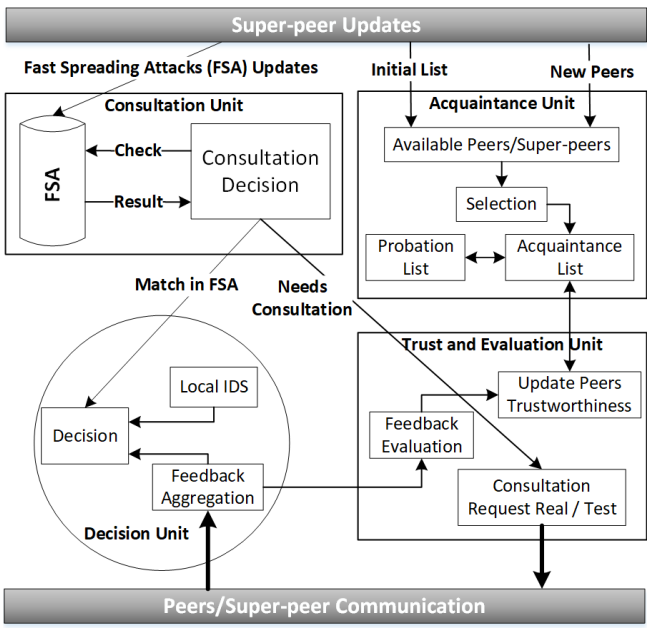

Fig. 2: The Proposed Architecture

3.2. Collaborators Responsibilities

As mentioned earlier, collaborators in the architecture fall into two types: peer and super-peer, both have similar responsibilities, but

the super-peer has some additional responsibilities which are going to be discussed in detail in this section.

3.2.1. Peers

Peers in the CIDN are organized based on their scope. A new peer is required to get the super-peer's approval to join a group in the CIDN that consists of peers that have the same scope. Once the request is approved, the new peer will receive an initial list of peers for each group. After that, peers will be able to send consultations request to other peers with respect to the scope that the suspicious activity lies as shown in Algorithm 1 (lines 1-10). However, this new peer information will be sent to other peers by super-peer as an update. Therefore, each peer will have a list of available peers that can be added to a peer's acquaintance list when needed. The update might also contain information about peers that have left or have been removed from the list CIDN.
Once a peer obtains the list of peers, it chooses its acquaintance list from the available peers received from the super-peer. Note that at least one super-peer in each group is included in the acquaintance list. Then, the peer begins to evaluate other peers within the CIDN based on their scope from previous real consultation requests or test ones (lines 11-15).

Algorithm 1: Decision making in a peer

```
1:  while LacksKnowledge do
2:      if ReceivedBefore then
3:          Make decision
4:      else
5:          Send consultation requests to relevant group
6:          Aggregate feedback
7:          Make decision
8:          Update peers' trust values
9:      end if
10: end while
11: while TestCR do
12:     Send test consultation request for known attack
13:     Compare feedback with local answer
14:     Update peers' trust values
15: end while
```

3.2.2. Super-Peers

A super-peer is responsible for registering new peers within its group (scope) as shown in Algorithm 2 (lines 1-7). It maintains a list of all peers and super-peers inside its group and the initial acquaintance list to be delivered to new registered peer in addition to maintaining the updated lists from other super-peers. Super-peer is operated and managed by security expert (a security firm or an organization). The information of the groups is exchanged and updated between super-peers, including initial acquaintance list of each group in addition to new available peers.
The super-peer employment in the architecture detects fast-spreading attacks based on consultation requests for similar suspicious activities within their group. Once the detected attack is confirmed, the information about it will be distributed to other group members (lines 9-24) and thus, helps reducing future consultation requests for this attack and increase efficiency for detecting these attacks. However, in this architecture, peers are free to consult other peers on different group scopes based on the consultation area, unlike the file-sharing super-peer that allow peers to only request from their super-peer. Peers that have low trustworthiness value will be removed of the available lists by super-peers.

Algorithm 2: Super-peer role in CIDN

```
1:  while NewPeerJoins do
2:      Determine peer's scope
3:      if Approved then
4:          Send the available peers list
5:          Add this peer to the available peers list
6:          Send this peer's info to other peers as an update
7:      end if
8:  end while
9:  while ConsultationRequest(CR)Received do
10:     if ReceivedBefore then
11:         Record Time
12:         Calculate time difference between this CR and previous one
13:         Quantify CR
14:         Update current value
15:         if ThresholdReached then
16:             List in fast spreading attacks (FSA)
17:             Send an update about this FSA to peers
18:         end if
19:     else
20:         Give an ID
21:         Record Time
22:         Quantify CR
23:     end if
24: end while
```

3.2.3. Groups

CIDSs have different platforms and strengths in various scopes that if exploited properly, they can strengthen the efficiency of the CIDN as well as reducing the overhead of the communication traffic to inexpert peers which leads to the overall scalability enhancements of the architecture. This is achieved in the proposed architecture, by organizing collaborators into several groups based on their scopes (area of expertise) regardless of their physical locations. These groups are known before operating the CIDN. Consequently, if a peer wants to consult about a suspicious activity, it consults the members of the group that is specialized in that scope. An example of these areas of expertise are Windows/Linux web server, Web App attacks, etc.

4. Scalability Analysis and Evaluation Discussion

In this section, the scalability of the proposed architecture will be evaluated and compared to the unstructured P2P architecture.
Several simulation scenarios have been conducted to see the impact of the proposed architecture in CIDN. However, A set of attack signatures has been created to be used in the simulation. As mentioned in pervious sections, fast-spreading attacks are detected and distributed to other peers among groups. We have created a list of fast-spreading attacks that is a subset of the attack signatures which is selected randomly based on the percentage stated in Table 1. This subset is distributed among all peers in our super-peer architecture and before a peer makes the decision to consult, it first checks this list to see whether or not there is a match. Each scenario consists of a number of simulated attacks that is selected randomly from the attack signatures.
Table 1 shows the simulations settings of various scenarios both structured and unstructured peer-peer environments using 10% and 20 % fast-spreading attacks (FSA) knowledge in each peer.

Table 1: Simulation Scenarios

	Attack Sig.	FSA Subset	Sim. Attacks	Peers	Groups	Peers in a Group
1	100	-	500	100	-	-
2	100	10%	500	100	4	25
3	100	20%	500	100	4	25
4	200	-	1000	150	-	-
5	200	10%	1000	150	5	30
6	200	20%	1000	150	5	30

In scenarios 2 and 3 (Table 1), 100 peers were divided into four groups. Each group (scope) consists of 25 peers specialized in one area of expertise (scope). While scenario 1 represents the normal unstructured peer-to-peer (P2P) which has no group or FSA knowledge. The results in Table 2 show how the consultation decisions decreased as the number of discovered fast-spreading attacks increases. There is a drop in the total consultation requests by 12% and 21% for super-peer (SP) architecture when having 10% and 20% FSA knowledge respectively. In P2P, about 75% of the total CRs were sent to inexpert peers (non-relevant group) which might cause high possibility of degraded efficiency, while only 25% CRs were sent to expert peers (relevant group).
Another set of simulation results in Table 2 consists of more simulated attacks, and more peers that are organized into five groups also shows a decrease by 9% and 15% in super-peer SP architecture with 10% and 20% FSA knowledge, respectively. The total number of CRs that are sent to the inexpert peers is 81%, which is much higher than the previous scenario, and the CRs sent to expert peers is 19%, which is lower than the previous one.

Table 2: Simulation Results for Scenarios 1, 2, and 3

CIDN	P2P	SP & 10% FSA	SP & 20% FSA
Consultation Decisions	500	456	411

Decisions obtained from FSA	0	44	89
Total CRs sent	12500	10944	9864
CRs sent reduction	0%	-12%	-21%
Total feedbacks received	12500	10944	9864
Feedbacks reduction	0%	-12%	-21%
CRs sent to relevant group	25%	100%	100%
Feedbacks from relevant group	25%	100%	100%
CRs sent to non-relevant group	75%	0%	0%
Feedbacks from non- relevant group	75%	0%	0%

Table 3: Simulation Results for Scenarios 4, 5, and 6

CIDN	P2P	SP & 10% FSA	SP & 20% FSA
Consultation Decisions	1000	944	881
Decisions obtained from FSA	0	56	119
Total CRs sent	30000	27376	25549
CRs sent reduction	0%	-9%	-15%
Total feedbacks received	30000	27376	25549
Feedbacks reduction	0%	-9%	-15%
CRs sent to relevant group	19%	100%	100%
Feedbacks from relevant group	19%	100%	100%
CRs sent to non-relevant group	81%	0%	0%
Feedbacks from non- relevant group	81%	0%	0%

Fig. 3 shows how the number of consultations is reduced as the number of fast-spreading attacks discovered increases in super-peer with 10% and 20% FSA knowledge.

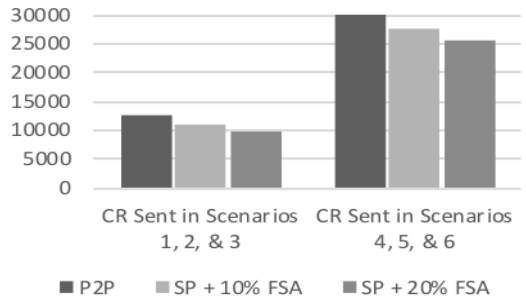

Fig. 3: The Number of Consultation Requests is Reduced as the Number of Discovered Fast-Spreading Attacks (FSA) Increases

From previous scenarios we can conclude that the architecture shows a positive impact in the overall scalability and efficiency, which are achieved by adopting the super-peer approach that organizes peers into the right group of expertise, and subsequently limits the consultation requests only to be sent to the group members that are good in their area of expertise. The impact on scalability and efficiency is improved when adopting the super-peer concept giving a more reliable results comparing to the unstructured P2P settings.

5. Conclusion

In this paper, we have presented our super-peer architecture that divides collaborators into groups based on their scope by employing the super-peer concept to enhance the scalability and the ability to accommodate more peers, without losing the control of the CIDN or creating a single point of failure. Moreover, this also strengthen the efficiency of the CIDN by reducing the chances of consulting inexpert peers and thus, affecting the decision that a CIDS makes. Also, our super-peer architecture facilitates the information-based incorporation into consultation-based CIDN by limiting the information being distributed to fast-spreading attacks or the severe ones that have been discovered from consultation requests.

Our future work is to develop an algorithm to detect fast-spreading attacks based on the consultation requests received from group members for the same suspicious activity to extend the capability of consultation-based CIDN to have some information-based benefits. The discovered attacks reflect that they are either new attacks or overlooked ones, and as a result, bringing the attention of group's members to these attacks that are taking place recently in this group. We are also interested to propose an acquaintance management algorithm to handle super-peers' roles in the architecture.

Acknowledgement

This material is partly based upon work supported by the Universiti Putra Malaysia under Grant No. GP/2018/9621600.

References

[1] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and Survey of Collaborative Intrusion Detection," ACM Computing Surveys (CSUR), vol. 47, no. 4, pp. 55, 2015.

[2] C. J. Fung and R. Boutaba, "Design and management of collaborative intrusion detection networks," in Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on, 2013, pp. 955-961

[3] L. Liu and N. Antonopoulos, "From client-server to p2p networking," in Handbook of Peer-to-Peer Networking, ed: Springer, 2010, pp. 71-89.

[4] Van Steen, M. and A. S. Tanenbaum, Distributed Systems. CreateSpace, 2017.

[5] Kurve, Aditya, et al. "Optimizing cluster formation in super-peer networks via local incentive design." Peer-to-Peer Networking and Applications 8.1 (2015): 1-21.

[6] L. Mekouar, Y. Iraqi, and R. Boutaba, "Reputation-based trust management in peer-to-peer systems: taxonomy and anatomy," in Handbook of Peer-to-Peer Networking, ed: Springer, 2010, pp. 689-732.

[7] R. Janakiraman, M. Waldvogel, and Q. Zhang, "Indra: A peer-to-peer approach to network intrusion detection and prevention," in Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on, 2003, pp. 226-231.

[8] V. Yegneswaran, P. Barford, and S. Jha, "Global Intrusion Detection in the DOMINO Overlay System," in NDSS, 2004.

[9] A. Ghosh and S. Sen, Agent-based distributed intrusion alert system: Springer, 2005.

[10] C. V. Zhou, S. Karunasekera, and C. Leckie, "A peer-to-peer collaborative intrusion detection system," 2005, p. 6 pp.

[11] C. Duma, M. Karresand, N. Shahmehri, and G. Caronni, "A trust-aware, p2p-based overlay for intrusion detection," in Database and Expert Systems Applications, 2006. DEXA'06. 17th International Workshop on, 2006, pp. 692-697.

[12] A. K. Ganame, J. Bourgeois, R. Bidou, and F. Spies, "A global security architecture for intrusion detection on computer networks," computers & security, vol. 27, pp. 30-47, 2008.

[13] C. V. Zhou, C. Leckie, S. Karunasekera, and T. Peng, "A self-healing, self-protecting collaborative intrusion detection architecture to trace-back fast-flux phishing domains," 2008, pp. 321-327.

[14] C.-C. Lo, C.-C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," 2010, pp. 280-284.

[15] M. G. Pérez, F. G. Mármol, G. M. Pérez, and A. F. S. Gómez, "RepCIDN: A reputation-based collaborative intrusion detection network to lessen the impact of malicious alarms," Journal of network and systems management, vol. 21, pp. 128-167, 2013.

[16] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," Network and Service Management, IEEE Transactions on, vol. 8, pp. 79-91, 2011.

[17] C. Fung, J. Zhang, I. Aib, and R. Boutaba, "Trust management and admission control for host-based collaborative intrusion detection," Journal of Network and Systems Management, vol. 19, pp. 257-277, 2011.

[18] W. Li, W. Meng, and H. Horace, "Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model," Journal of Network and Computer Applications, vol. 77, pp. 135-145, 2017.