A SUPER-PEER ARCHITECTURE TO IMPROVE INTRUSION DETECTION AND SCALABILITY IN COLLABORATIVE INTRUSION DETECTION NETWORK

YOUSEF ABDULLAH BAKHDLAGHI

FSKTM 2020 15

A SUPER-PEER ARCHITECTURE TO IMPROVE INTRUSION DETECTION AND SCALABILITY IN COLLABORATIVE INTRUSION DETECTION NETWORK

By

YOUSEF ABDULLAH BAKHDLAGHI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

June 2020

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

A SUPER-PEER ARCHITECTURE TO IMPROVE INTRUSION DETECTION AND SCALABILITY IN COLLABORATIVE INTRUSION DETECTION NETWORK

By

YOUSEF ABDULLAH BAKHDLAGHI

June 2020

Chair:	**Nur Izura Udzir, PhD**
Faculty:	**Computer Science and Information Technology**

Collaborative intrusion detection network (CIDN) offers the ability to correlate suspicious activities from various collaborative intrusion detection systems (CIDSs) in different networks to maximize the efficiency of the intrusion detection by sharing the knowledge and resources among them which facilitates the discovery of large-scale and coordinated attacks. Although existing CIDN offers consultation capability for collaborators when a single CIDS lacks knowledge about a security event, it does not consider the collaborators' attack scopes when requesting for consultation which can result in consulting inexpert peers and thus, degrade the efficiency of intrusion detection in CIDN and negatively affect the scalability of the CIDN, while in reality CIDSs have different strengths in various attack areas. In addition, fast-spreading attack (FSA) is one of the most serious threats in the networked environments that can infect hosts and propagate in an exponential rate in a short period of time. This type of attack might spread across the nodes and overwhelm the CIDN with consultation requests due to the lack of a mechanism to discover FSA from consultation requests in the CIDN. In fact, these consultation requests have not been utilized yet to detect FSA in existing CIDN architectures.

The aim of this study is to propose a scope-aware super-peer CIDN architecture as well as detecting FSA based on consultation requests that occur within CIDN. A statistical approach called exponentially weighted moving average (EWMA) is proposed with adaptive threshold to detect fast-spreading attacks (anomaly) in CIDN. The effectiveness of the proposed architecture has been evaluated through a discrete-event simulation under different intrusion detection measurements in terms of detection accuracy, FSA detection, and scalability with flexibility in adjusting simulation parameters to perform different test scenarios in the CIDN and compare the proposed super-peer CIDN architecture with the previous unstructured peer-to-peer architecture. Several simulation scenarios were performed for evaluating the performance of the proposed super-peer architecture. The simulation results demonstrate the feasibility of the proposed architecture and showed an improved performance in various intrusion detection metrics, including true-positive rate (TPR), true-negative rate (TNR), false-positive rate (FPR), false-negative rate (FNR), detection accuracy (DA), receiver operating characteristic (ROC), FSA detection, and overall scalability. In fact, nodes in the super-peer CIDN architecture are able to obtain more reliable feedbacks and thus, a better intrusion detection compared to the previous peer-to-peer CIDN architecture. Additionally, the FSA detection and FSA knowledge-base employment in the architecture has shown an improvement in consultation requests and feedbacks reduction and improve the scalability of the proposed architecture. Therefore, the super-peer architecture is a better solution for CIDN to strengthen the efficiency of intrusion detection as CIDN scales up as well as reducing the overload of unnecessary consultation requests and feedbacks among collaborators which contributes to effectively enhance the overall scalability of the architecture.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk Ijazah Doktor Falsafah

SENI BINA SUPER-RAKAN UNTUK MENINGKATKAN PENGESANAN PENCEROBOHAN DAN SKALABILITI DALAM RANGKAIAN PENGESANAN PENCEROBOHAN KOLABORATIF

Oleh

YOUSEF ABDULLAH BAKHDLAGHI

Jun 2020

Pengerusi: **Nur Izura Udzir, PhD**

Fakulti: **Sains Komputer dan Teknologi Maklumat**

Rangkaian pengesanan pencerobohan kolaboratif (CIDN) menawarkan keupayaan untuk menghubungkaitkan aktiviti mencurigakan dari pelbagai sistem pengesanan pencerobohan kolaboratif (CIDS) dalam rangkaian yang berbeza untuk memaksimumkan kecekapan pengesanan pencerobohan dengan berkongsi pengetahuan dan sumber antara mereka yang memudahkan penemuan serangan berskala besar dan yang diselaraskan. Walaupun CIDN sedia ada menawarkan keupayaan perundingan untuk kolaborator ketika CIDS tunggal tidak memiliki pengetahuan tentang peristiwa keselamatan, ia tidak mempertimbangkan ruang lingkup serangan kolaborator ketika meminta perundingan yang dapat mengakibatkan konsultasi dengan rakan yang tidak pakar dan justeru, menurunkan kecekapan pengecaman pencerobohan CIDN dan secara negatifnya mempengaruhi skalabiliti CIDN, sedangkan pada kenyataannya CIDS mempunyai kekuatan yang berbeza dalam pelbagai kawasan serangan. Tambahan pula, serangan cepat menyebar (FSA) adalah salah satu ancaman paling serius dalam lingkungan jaringan yang boleh menjangkiti hos dan menyebarkan dengan kadar eksponen dalam jangka waktu yang singkat. Jenis serangan ini mungkin tersebar dalam kalangan nod dan membanjiri CIDN dengan permintaan perundingan akibat kurangnya mekanisme untuk menemukan FSA dari permintaan perundingan dalam CIDN. Malah, permintaan perundingan ini belum digunakan untuk mengesan FSA dalam seni bina CIDN sedia ada.

Tujuan kajian ini adalah untuk mengusulkan seni bina CIDN super-rakan yang peka skop serta mengesan FSA berdasarkan permintaan perundingan yang berlaku dalam CIDN. Pendekatan statistik yang disebut purata bergerak berwajaran eksponen (EWMA) diusulkan dengan ambang batas adaptif untuk mengesan serangan cepat menyebar (anomali) dalam CIDN. Keberkesanan seni bina yang dicadangkan ini telah dinilai melalui simulasi peristiwa diskrit di bawah pengukuran pengesanan pencerobohan yang berbeza dari segi ketepatan pengesanan, pengesanan FSA, dan skalabiliti dengan fleksibiliti dalam menyesuaikan parameter simulasi untuk melakukan senario ujian yang berbeza dalam CIDN dan membandingkan seni bina CIDN super-rakan yang dicadangkan dengan seni bina rakan-ke-rakan sebelumnya yang tidak berstruktur. Beberapa senario simulasi dilakukan untuk menilai prestasi seni bina super-rakan yang dicadangkan. Hasil simulasi menunjukkan kebolehlaksanaanseni bina yang dicadangkan dan menunjukkan peningkatan prestasi dalam pelbagai metrik pengesanan pencerobohan, termasuk kadar positif-benar (TPR), kadar negatif-benar (TNR), kadar positif-palsu (FPR), kadar negatif-palsu (FNR), ketepatan pengesanan (DA), ciri operasi penerima (ROC), pengesanan FSA, dan skalabiliti keseluruhan. Malah, nod dalam seni bina CIDN super-rakan berupaya memperoleh maklum balas yang lebih dipercayai dan dengan itu, menghasilkancpengesanan pencerobohan yang lebih baik berbanding dengan seni bina CIDN rakan-ke-rakan terdahulu. Selain itu, pengesanan FSA dan penggunaan berasaskan pengetahuan FSA dalam seni bina telah menunjukkan peningkatan dalam permintaan perundingan dan pengurangan maklum balas dan yang meningkatkan skalabiliti seni bina yang dicadangkan. Oleh itu, seni bina super-rakan adalah penyelesaian yang lebih baik bagi CIDN untuk memperkukuh kecekapan pengesanan pencerobohan ketika CIDN meningkat serta mengurangkan beban permintaan dan maklum balas perundingan yang tidak perlu dalam kalangan kolaborator yang menyumbang ke arah meningkatkan secara berkesan skalabiliti keseluruhan seni bina.

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation and deepest gratitude to my supervisor Associate Prof. Dr. Nur Izura Udzir and my supervisory committee members Associate Prof. Dr. Azizol Abdullah, and Associate Prof. Dr. Nor Fazlida Mohd Sani for their valuable guidance and advice throughout my research journey at UPM.

Most of all, I would like to express my sweetest appreciation to my family for their patience and endless support. Their prayers and wishes constantly helped me to be strong and encouraged me to achieve the PhD.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy.

The members of the Supervisory Committee were as follows:

Nur Izura Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Azizol Abdullah, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Nor Fazlida Mohd Sani, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 10 September 2020

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ___________________
Name of Chairman of Supervisory Committee:
Nur Izura Udzir

Signature: ___________________
Name of Member of Supervisory Committee:
Azizol Abdullah

Signature: ___________________
Name of Member of Supervisory Committee:
Nor Fazlida Mohd Sani

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF NOTATIONS

$\mathcal{N}$	the set of all nodes
$\vert\mathcal{N}\vert$	the number of nodes in set $\mathcal{N}$
$\mathcal{N}^j$	the nodes in group j ($\mathcal{N}^j \subseteq \mathcal{N}$)
$\mathcal{D}$	the dataset of generated attacks
$\vert\mathcal{D}\vert$	the number of records in set $\mathcal{D}$
$\overline{\mathcal{D}}$	dataset that includes $\mathcal{D}$ and fast-spreading according to α_1 , α_2 parameters
$\mathcal{D}_k$	a subset of the dataset $\mathcal{D}$ ($\mathcal{D}_k \subseteq \mathcal{D}$) that consists of all attack categories k
$\vert\mathcal{D}_k\vert$	the number of records in subset $\mathcal{D}_k$
$\mathcal{S}^j$	represents fast-spreading attack knowledge in group j ($\mathcal{S}^j \subseteq \mathcal{D}_k$)
$\vert\mathcal{S}^j\vert$	the number of records in subset $\mathcal{S}^j$, where $\vert\mathcal{S}^j\vert = a_1 \times \vert\mathcal{D}_k\vert$
N	the number of nodes in the CIDN
Y	holds feedbacks from nodes
$\delta\,(Y)$	the decision based on feedbacks Y
λ	the intensity of interarrival time in Piosson process
A	interarrival time
t	current simulation time, $t_0 = 0$, $t_1 = t_0 + A_1$
p	success (attack) rate in Bernoulli process
k	an attack category
m	the number of groups in the CIDN
n	the number of nodes in each group
a_1	the percentage of which fast-spreading attacks are generated from the records in each group $\mathcal{S}^j$, where $\vert\mathcal{S}^j\vert = a_1 \times \vert\mathcal{D}_k\vert$ and $k \in$ group j
a_2	the percentage of $\mathcal{S}^j$ to consider for reoccurrence
x	the number of reoccurrence of an attack
c	a consultation request
d	a record from the dataset $\mathcal{D}$

LIST OF ABBREVIATIONS

AAWP	Analytical Active Worm Propagation
C2	Command and Control
CIA	Confidentiality, Integrity, and Availability
CIDN	Collaborative Intrusion Detection Network
CIDS	Collaborative Intrusion Detection System
CR	Consultation Request
DA	Detection Accuracy
DoS	Denial-of-service Attack
EWMA	Exponentially Weighted Moving Average
FN	False Negative
FNR	False Negative Rate
FP	False Positive
FPR	False Positive Rate
FSA	Fast-spreading Attack
HIDS	Host-based Intrusion Detection System
IDMEF	Intrusion Detection Message Exchange Format
IDS	Intrusion Detection System
MITM	Man-in-the-middle Attack
MV	Majority Vote
NIDS	Network-based Intrusion Detection System
P2P	Peer-to-peer
PKI	Public Key Infrastructure
RFC	Request for Comments
ROC	Receiver Operating Characteristic
SP	Super-peer
SSJ	Stochastic Simulation in Java
STIX	Structured Threat Information Expression
TN	True Negative
TNR	True Negative Rate
TP	True Positive
TPR	True Positive Rate

GLOSSARY OF TERMS

#	Term	Definition
1	Confusion Matrix	A table to visualize the performance of intrusion detection that distinguish the normal and malicious instances in both, actuality, and predicted results (Hamed et al., 2017).
2	Cyber-attack	Cyber-attack is a malicious attempt that targets information systems, computers, computer networks, or infrastructures, aims at disrupting the CIA triad (Confidentiality, Integrity, and Availability) of information security (Narwal et al., 2019).
3	Exploit	A piece of code that takes advantage of a single or multiple vulnerabilities (Stallings and Brown, 2018).
4	Intrusion Detection	A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner (Stallings and Brown, 2018).
5	Malicious Code	Refers to malware or malicious software which includes viruses, worms, and any software that its purpose is to attack a platform (Nieles et al., 2017).
6	Malware	Malware is a term for all malicious software or code that is specifically designed to gain access or cause damage to a device or a computer network, usually without the victim's knowledge.
7	Node	In graph theory, a node is the fundamental unit that forms the graph. Nodes are connected by a communication network that collaborate to perform specific tasks (Erciyes, 2013). In this thesis, the terms peer, super-peer, CIDS, and collaborators are interchangeably referring to node.

8	Receiver Operating Characteristics	A graphical plot that illustrates the trade-off between true positive rate (TPR) against false positive rate (FPR) (Powers, 2011).
9	Security Compromise	A security violation of a system that potentially could leave the system exposed to unauthorized access or attack (Shirey, 2007).
10	Security Event	An occurrence in a system, service, or network that is relevant to security (Shirey, 2007).
11	Security Incident	A security event that may indicates a violation of information, computer, or network security (Shirey, 2007).
12	Security Intrusion	A security event, or a combination of security events, that from a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so (Stallings and Brown, 2018).
13	Vulnerability	A term that refers to a flow or weakness in a computer system that potentially could leave the system exposed to attacks (Symantec, 2019).

CHAPTER 1

INTRODUCTION

1.1 Motivation

Technology has changed our way of communication and revolutionized our lives in ways that eliminate time and distance barriers with its continuous advances over years. There is no doubt that the usage of Internet for online transactions has been raised dramatically and become an integral part of people's life across the globe. Unfortunately, this potentially expose people's online activities (including governments, banks, and organizations online services) to hackers who have malicious intentions to gain access, destruct, or make a profit from such intrusions.

An alarming report from Risk Based Security (RBS, 2019) shows how the number of disclosed vulnerabilities has increased noticeably in the past five years (Figure 1.1).

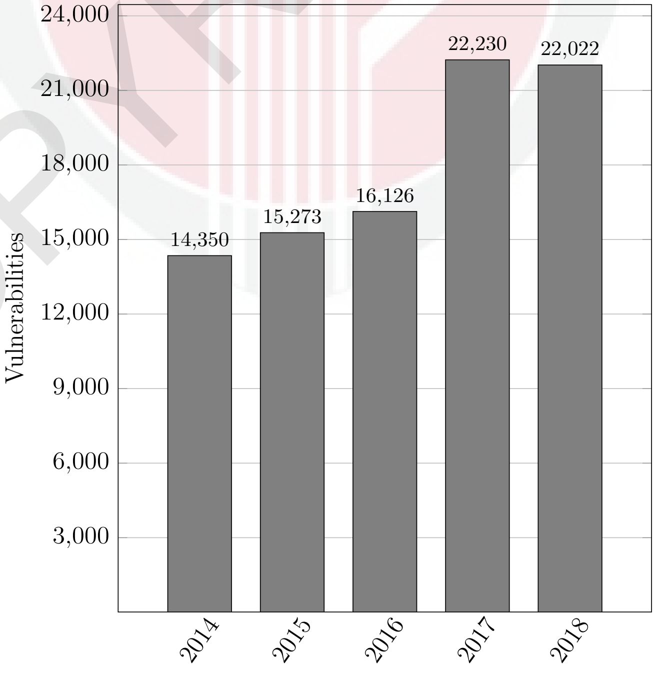

Figure 1.1: The Number of Vulnerabilities Disclosed, 2014-2018 (RBS, 2019)

These vulnerabilities give a sign of growing threats that require continuous improvements and developments of countermeasure systems. In particular, more than 22,000 security vulnerabilities were disclosed in 2018 and 2019; 33% of the disclosed vulnerabilities in 2018 are rated as severe (RBS, 2019). In fact, the cost of cybercrime is estimated to grow annually from $3 trillion in 2015 to $6 trillion by the end of 2021 (K. Huang et al., 2018). Consequently, cybersecurity remains a complex challenge for businesses and end-users worldwide in the Internet (Thames, 2014).

Figure 1.2 shows the growing threat of cyber-attacks in Malaysia from year 2005 to 2018, according to reported incidents to Malaysia Computer Emergency Response Team (MyCERT, 2019). In fact, the number of the reported incidents has increased remarkably for the past 15 years.

The importance of combating cyber-attacks and intrusions has led researchers to develop a collaboration between IDS to extends a single IDS's detection capability for discovering new threats and attacks. As a result, collaborative intrusion detection network (CIDN) has been introduced to address that.

Collaborative intrusion detection network (CIDN) offers 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 to facilitate the discovery of large-scale and coordinated attacks (Li and Kwok, 2019) (Vasilomanolakis et al., 2015). CIDN falls into two categories: information-based and consultation-based CIDN. The information-based CIDN allows collaborators to share their knowledge and observation. It enables an IDS to alert others about intrusions and attacks. On the other hand, consultation-based CIDN is an on-demand collaboration that is used when an IDS lacks knowledge and confidence about a suspicious activity or a security event (Vasilomanolakis et al., 2015) (Fung and Boutaba, 2013).

As cyber-attacks become large-scaled and more destructive, defending against such attacks is extremely important which requires further security approaches to countermeasure such attacks. One promising approach that extends a single IDS's capability is the CIDN. This approach allows an IDS to collaborate with multiple intrusion detection systems for knowledge-sharing and better intrusion detection.

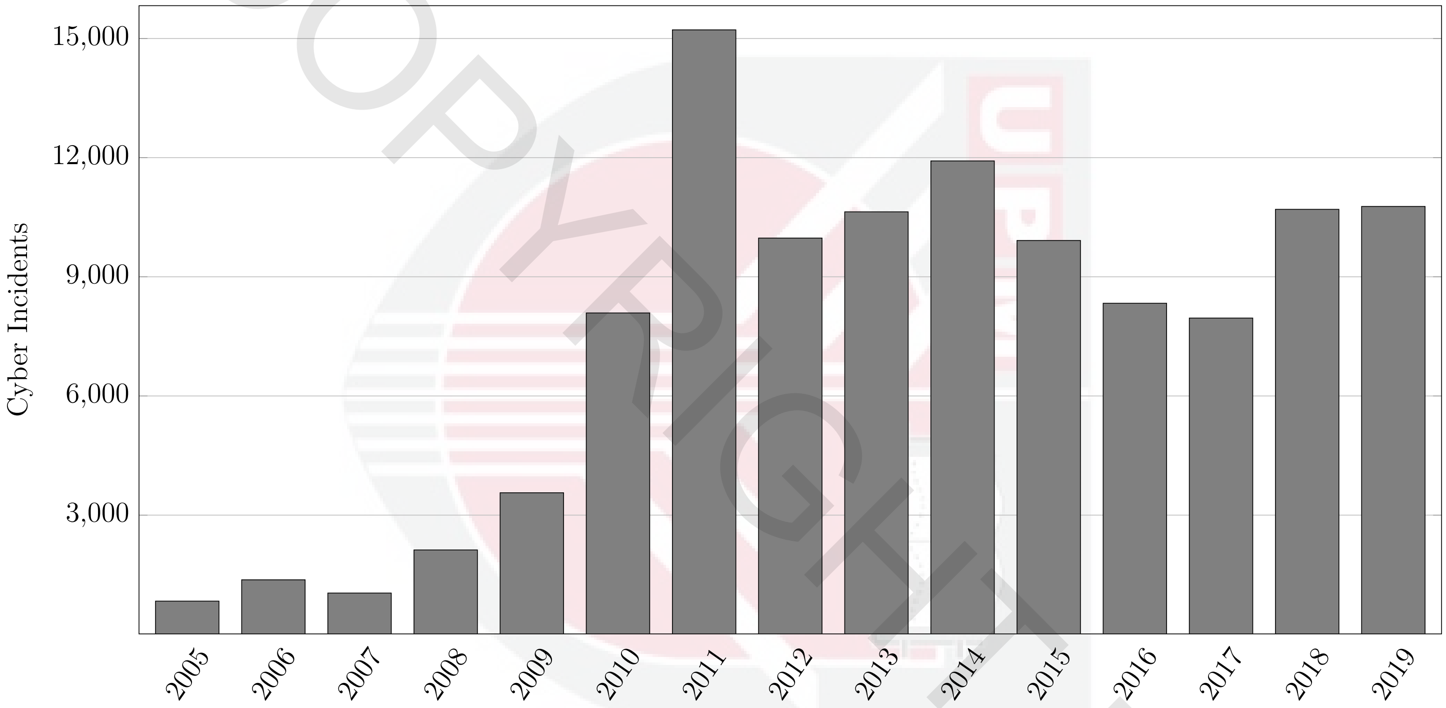

Figure 1.2: The Number of Reported Cyber Incidents in Malaysia, 2005-2018

The field of collaborative security, including intrusion detection, is attracting more attention recently with continuous efforts to enhance the collaboration and intrusion detection, but "*the success of collaborative security relies on not only its ability to address the challenges of traditional security but also the accuracy and efficiency of security analysis*" (G. Meng et al., 2015). Yet, there is no scalable solution in the literature for carrying out collaborative intrusion detection in large networks (Vasilomanolakis et al., 2015). Consequently, the necessity for continuous enhancement of intrusion detection and IDS's collaboration capabilities is the motivation for this research.

1.2 Problem Statement

Existing consultation-based CIDN architecture does not address the scope variations of CIDSs. Consulting nodes without considering scope variations could affect the efficiency of the CIDN and increase the overload of unnecessary consultation requests to inexpert peers which poses scalability issues as the CIDN scales up. Additionally, there is no mechanism in the existing consultation-based CIDN to monitor these consultation requests for the presence of fast-spreading attacks (FSA).

Particularly, this thesis addresses the following issues:

1. Current consultation-based CIDN does not address the variations of CIDSs scopes, consulting nodes without considering their scope variations could degrade the efficiency of the CIDN, and increase the overload of unnecessary consultation requests to inexpert peers, requesting and responding, which affects the decision made by a CIDS as well as affecting the overall scalability of the architecture. Additionally, there is no scalable solution in the literature for carrying out collaborative intrusion detection in large networks (Vasilomanolakis et al., 2015).

2. One of the most serious threats in the networked environments is fast-spreading attacks. This kind of attacks have a self-propagation capabilities that can infect hosts and propagate in an exponential rate, affecting millions of hosts in a short period of time (Bardhan et al., 2019) (Boukerche and Zhang, 2019) (O'Brien, 2017) (Lan Liu et al., 2017) (Dua and Du, 2016) (S. Chen et al., 2014). Existing CIDN offers consultation capability without having a mechanism to monitor

these consultation requests for detecting FSA. However, consultation requests from several CIDSs for the same security event in a short period of time could be a sign of FSA that if not detected, the same attack might spread and target other nodes, which can affect the intrusion detection and the scalability of the CIDN. Also, existing consultation requests within CIDN have not been utilized yet to discover such attacks.

1.3 Research Objectives

The main research objective of this research is to propose a super-peer collaborative intrusion detection network (CIDN) for better intrusion detection and scalability.

The detailed objectives are:

1. to propose a scope-aware architecture to increase the efficiency and scalability of CIDN by organizing CIDN peers into groups based on their scope to reduce unnecessary consultation requests sent to inexpert peers and facilitate obtaining initial peers list and updates.

2. to propose a mechanism for detecting fast-spreading attacks for the proposed super-peer CIDN architecture and prevent the spreading of fast spreading attacks and enhance detection accuracy and scalability.

1.4 Research Scope

This research focuses on enhancing the scalability and the efficiency of consultation-based collaborative intrusion detection network (CIDN) which evaluated through stochastic simulation method that acquired data from statistical distributions and mathematical models. However, the decision when to consult, the communication between collaborators, insider attacks and attacks against the CIDN itself are not covered in this research scope.

1.5 Research Contributions

The major contribution of this research is the proposal of a super-peer collaborative intrusion detection network (CIDN) architecture to enhance intrusion detection efficiency and scalability of the CIDN.

The detailed contributions of this research are:

1. A new scalable super-peer CIDN architecture that contribute to enhance detection accuracy and scalability as well as facilitating FSA detection in the architecture. Simulations show remarkable improvements in detection accuracy and scalability comparing to existing peer-to-peer CIDN.

2. A mechanism to detect fast-spreading attacks (FSA) for super-peer collaborative intrusion detection network (CIDN) using statistical anomaly detection method (EWMA) to monitor the intensity of consultation requests in CIDN that reflects FSA. This mechanism has shown an enhancement to detection accuracy, intrusion detection and scalability.

1.6 Thesis Organization

This thesis is organized in eight chapters as follows:

Chapter 1 provides an outline of the study, including research background, motivation, problem statement, research objectives, research scope and research contributions.

Chapter 2 presents an overview of cyber-attacks, intrusion detection, and collaborative intrusion detection. Then, reviews the related work and challenges in both collaborative intrusion detection networks (CIDN) and statistical-based anomaly detection, finding gaps and limitations in existing work.

Chapter 3 elaborates the methodology used in this research including requirement analysis, designing the proposed architecture, simulation design, and evaluation. It investigates the current CIDN limitations, find the gaps and propose the solution. Then, provides the simulation design, evaluation criteria and result analysis for the proposed solution.

Chapter 4 describes the proposed scope-aware super-peer collaborative intrusion detection network (CIDN) architecture in detail. A comprehensive description of its components and organization are provided.

Chapter 5 presents the proposed mechanism for detecting fast-spreading attacks in the consultation-based CIDN through statistical-based anomaly detection to detect the intensity of consultation requests.

Chapter 6 focuses on the simulation design and evaluation of the proposed architecture in terms of detection accuracy and scalability. A discrete-event simulation is used to evaluate the super-peer CIDN architecture and compare it to unstructured peer-to-peer CIDN architecture using various statistical distribution, such as Poisson and Bernoulli distribution that assist in the architecture evaluation.

Chapter 7 illustrates the performance evaluation of the super-peer CIDN architecture and the fast-spreading attacks detection based on various evaluation criteria described in Chapter 3.

Chapter 8 concludes the entire thesis with highlights on its findings of the proposed architecture and recommends some potential future work of this research.

REFERENCES

Akujobi, F., Lambadaris, I., & Kranakis, E. (2007). *Endpoint-driven intrusion detection and containment of fast spreading worms in enterprise networks.* Paper presented at the Military Communications Conference, 2007. MILCOM 2007. IEEE.

Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science, 25*, 152-160.

Amoli, P. V., Hamalainen, T., David, G., Zolotukhin, M., & Mirzamohammad, M. (2016). Unsupervised network intrusion detection systems for zero-day fast-spreading attacks and botnets. *Int. J. Digit. Content Technol. Its Appl, 10*(2), 1-13.

Bardhan, S., Montgomery, D. C., Filliben, J. J., & Heckert, N. A. (2019). A General Methodology for Deriving Network Propagation Models of Computer Worms. Retrieved 27 Oct, 2019, from https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2035.pdf

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2013). Network anomaly detection: methods, systems and tools. *IEEE Communications Surveys & Tutorials, 16*(1), 303-336.

Bojović, P., Bašičević, I., Ocovaj, S., & Popović, M. (2019). A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. *Computers & Electrical Engineering, 73*, 84-96.

Boukerche, A., & Zhang, Q. (2019). Countermeasures against Worm Spreading: A New Challenge for Vehicular Networks. *ACM Computing Surveys (CSUR), 52*(2), 34.

Bouyeddou, B., Harrou, F., Sun, Y., & Kadri, B. (2017). *Detecting SYN flood attacks via statistical monitoring charts: A comparative study.* Paper presented at the 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B).

Burt, A. L., Darschewski, M., Ray, I., Thurimella, R., & Wu, H. (2008). Origins: an approach to trace fast spreading worms to their roots. *International Journal of Security and Networks, 3*(1), 36-46.

Chadd, A. (2018). DDoS attacks: past, present and future. *Network Security, 2018*(7), 13-15.

Chen, S., Liu, L., Wang, X., Zhang, X., & Zhang, Z. (2014). A host-based approach for unknown fast-spreading worm detection and containment. *ACM Transactions on Autonomous and Adaptive Systems (TAAS), 8*(4), 21.

Chen, Z., Gao, L., & Kwiat, K. (2003). *Modeling the spread of active worms*.

Čisar, P., & Čisar, S. M. (2019). Ewma Statistics And Fuzzy Logic In Function Of Network Anomaly Detection. *Facta Universitatis, Series: Electronics and Energetics, 32*(2), 249-265.

Cordero, C. G., Traverso, G., Nojoumian, M., Habib, S. M., Mühlhäuser, M., Buchmann, J., & Vasilomanolakis, E. (2018). Sphinx: a Colluder-Resistant Trust Mechanism for Collaborative Intrusion Detection. *IEEE Access, 6*, 72427-72438.

Danyliw, R., Meijer, J., & Demchenko, Y. (2007). RFC5070-The Incident Object Description Exchange Format. *Internet Engineering Task Force (IETF)*.

Darley, T., Struse, R., & Ginn, J. (2017). Structured Threat Information eXpression (STIX): Version 2.0. Retrieved Oct 10, 2019, from https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.pdf

Debar, H., Curry, D., & Feinstein, B. (2007). RFC4765: The Intrusion Detection Message Exchange Format (IDMEF). *The Internet Engineering Task Force (IETF)*.

Di, M. (2019). *Design of the Network Security Intrusion Detection System Based on the Cloud Computing.* Paper presented at the The International Conference on Cyber Security Intelligence and Analytics.

Diibendorfer, T., & Plattner, B. (2005). *Host behaviour based early detection of worm outbreaks in internet backbones.* Paper presented at the 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05).

Ding, D., Han, Q.-L., Xiang, Y., Ge, X., & Zhang, X.-M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing, 275*, 1674-1683.

Dua, S., & Du, X. (2016). *Data mining and machine learning in cybersecurity*: Auerbach Publications.

Duma, C., Karresand, M., Shahmehri, N., & Caronni, G. (2006). *A trust-aware, p2p-based overlay for intrusion detection.* Paper presented at the 17th International Workshop on Database and Expert Systems Applications (DEXA'06).

Erciyes, K. (2013). *Distributed graph algorithms for computer networks*: Springer Science & Business Media.

Fachkha, C., & Debbabi, M. (2016). Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. *IEEE Communications Surveys & Tutorials, 18*(2), 1197-1227.

Feng, K., Gu, X., Peng, W., & Yang, D. (2019). *Moving Target Defense in Preventing SQL Injection*, Cham.

Folino, G., & Sabatino, P. (2016). Ensemble based collaborative and distributed intrusion detection systems: A survey. *Journal of Network and Computer Applications, 66*, 1-16.

Fung, C. J., & Boutaba, R. (2013). *Design and management of collaborative intrusion detection networks.* Paper presented at the 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013).

Fung, C. J., Zhang, J., Aib, I., & Boutaba, R. (2011). Dirichlet-based trust management for effective collaborative intrusion detection networks. *IEEE Transactions on Network and Service Management, 8*(2), 79-91.

Fung, C. J., Zhang, J., Aib, I., Boutaba, R., & Cohen, R. (2009). *Design of a simulation framework to evaluate trust models for collaborative intrusion detection.* Paper presented at the 2009 International Conference on Network and Service Security.

Fung, C. J., & Zhu, Q. (2016). FACID: A trust-based collaborative decision framework for intrusion detection networks. *Ad Hoc Networks, 53*, 17-31.

Ganame, A. K., Bourgeois, J., Bidou, R., & Spies, F. (2008). A global security architecture for intrusion detection on computer networks. *Computers & Security, 27*(1), 30-47.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security, 28*(1-2), 18-28.

Ghosh, A., & Sen, S. (2005). *Agent-based distributed intrusion alert system*: Springer.

Gupta, A., & DuVarney, D. C. (2004). *Using predators to combat worms and viruses: A simulation-based study*.

Gupta, S., & Gupta, B. B. (2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management, 8*(1), 512-530.

Gyanchandani, M., Rana, J., & Yadav, R. (2012). Taxonomy of anomaly based intrusion detection system: a review. *International Journal of Scientific and Research Publications, 2*(12), 1-13.

Hamed, T., Dara, R., & Kremer, S. C. (2017). Intrusion Detection in Contemporary Environments *Computer and Information Security Handbook* (pp. 109-130): Elsevier.

Hoque, M. S., Mukit, M., Bikas, M., & Naser, A. (2012). An implementation of intrusion detection system using genetic algorithm. *arXiv preprint arXiv:1204.1336*.

Huang, K., Siegel, M., & Stuart, M. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR), 51*(4), 70.

Huang, Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A. C., & McCoy, D. (2018). *Tracking ransomware end-to-end.* Paper presented at the 2018 IEEE Symposium on Security and Privacy (SP).

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), 80.

ITRC. (2017). Identity Theft Resource Center - Breach Statistics 2005 - 2016. Retrieved Oct 21, 2019, from https://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf

ITRC. (2018). Identity Theft Resource Center - 2017 Annual Data Breach Year-End Review. Retrieved 21 Oct, 2019, from https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

Janakiraman, R., Waldvogel, M., & Zhang, Q. (2003). *Indra: A peer-to-peer approach to network intrusion detection and prevention.* Paper presented at the WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003.

Jin, R., He, X., & Dai, H. (2017). *On the tradeoff between privacy and utility in collaborative intrusion detection systems-a game theoretical approach.* Paper presented at the Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp.

Jyothsna, V., Prasad, V. R., & Prasad, K. M. (2011). A review of anomaly based intrusion detection systems. *International Journal of Computer Applications, 28*(7), 26-35.

Kammerdiner, A. R. (2014). Statistical techniques for assessing cyberspace security *Dynamics of Information Systems* (pp. 161-177): Springer.

Kurve, A., Griffin, C., Miller, D. J., & Kesidis, G. (2015). Optimizing cluster formation in super-peer networks via local incentive design. *Peer-to-Peer Networking and Applications, 8*(1), 1-21.

L'Ecuyer, P. (2016). SSJ: Stochastic Simulation in Java, Software Library. Retrieved Feb 3, 2020, from http://simul.iro.umontreal.ca/ssj/indexe.html and https://github.com/umontreal-simul/ssj

Law, A. M., & Kelton, W. D. (2014). *Simulation modeling and analysis* (5th ed.): McGraw-Hill New York.

Li, W., & Kwok, L. F. (2019). Challenge-based collaborative intrusion detection networks under passive message fingerprint attack: A further analysis. *Journal of Information Security and Applications, 47*, 1-7.

Li, W., Meng, W., Kwok, L. F., & Horace, H. (2017). Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. *Journal of Network and Computer Applications, 77*, 135-145.

Liu, L., & Antonopoulos, N. (2010). From client-server to p2p networking *Handbook of Peer-to-Peer Networking* (pp. 71-89): Springer.

Liu, L., Ko, R. K., Ren, G., & Xu, X. (2017). Malware propagation and prevention model for time-varying community networks within software defined networks. *Security and Communication Networks, 2017*.

Lo, C.-C., Huang, C.-C., & Ku, J. (2010). *A cooperative intrusion detection system framework for cloud computing networks*.

Machaka, P., Bagula, A., & Nelwamondo, F. (2016). *Using exponentially weighted moving average algorithm to defend against DDoS attacks.* Paper presented at the 2016 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech).

Man, N. D., & Huh, E.-N. (2012). *A collaborative intrusion detection system framework for cloud computing.* Paper presented at the Proceedings of the International Conference on IT Convergence and Security 2011.

Maxion, R. A., & Roberts, R. R. (2004). *Proper use of ROC curves in Intrusion/Anomaly Detection*: University of Newcastle upon Tyne, Computing Science.

Mekouar, L., Iraqi, Y., & Boutaba, R. (2010). Reputation-based trust management in peer-to-peer systems: taxonomy and anatomy *Handbook of Peer-to-Peer Networking* (pp. 689-732): Springer.

Meng, G., Liu, Y., Zhang, J., Pokluda, A., & Boutaba, R. (2015). Collaborative security: A survey and taxonomy. *ACM Computing Surveys (CSUR), 48*(1), 1.

Meng, W., Li, W., & Kwok, L. F. (2017). Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments. *IEEE Transactions on Network and Service Management, 14*(1), 233-245.

Meng, W., Luo, X., Li, W., & Li, Y. (2016). *Design and evaluation of advanced collusion attacks on collaborative intrusion detection networks in practice.* Paper presented at the 2016 IEEE Trustcom/BigDataSE/ISPA.

Mims, N. (2017). Chapter 84 - Cyber-Attack Process *Computer and Information Security Handbook (Third Edition)* (pp. 1105-1116): Morgan Kaufmann.

Montgomery, D. C. (2009). *Introduction to statistical quality control*: John Wiley & Sons (New York).

MyCERT. (2019). Malaysia Computer Emergency Response Team - Incident Statistics. Retrieved 30 Jan, 2020, from https://www.mycert.org.my

Nagar, U., Nanda, P., He, X., & Tan, Z. (2017). *A framework for data security in cloud using collaborative intrusion detection scheme*. Paper presented at the Proceedings of the 10th International Conference on Security of Information and Networks, Jaipur, India.

Narwal, B., Mohapatra, A. K., & Usmani, K. A. (2019). Towards a taxonomy of cyber threats against target applications. *Journal of Statistics and Management Systems, 22*(2), 301-325.

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). An Introduction to Information Security - NIST special publication 800-12 revision 1. National Institute of Standards and Technology (NIST). Retrieved 23 Sep, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Nisioti, A., Mylonas, A., Yoo, P. D., & Katos, V. (2018). From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods. *IEEE Communications Surveys & Tutorials, 20*(4), 3369-3388.

O'Brien, D. (2017). Internet Security Threat Report-Ransomware 2017. Symantec. Retrieved 28 Dec, 2019, from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf

Oberoi, P., & Mittal, S. (2018). *Review of CIDS and Techniques of Detection of Malicious Insiders in Cloud-Based Environment*. Springer, Singapore.

Pastrana, S., Tapiador, J. E., Orfila, A., & Peris-Lopez, P. (2015). DEFIDNET: A framework for optimal allocation of cyberdefenses in Intrusion Detection Networks. *Computer Networks, 80*, 66-88.

Pérez, M. G., Mármol, F. G., Pérez, G. M., & Gómez, A. F. S. (2013). RepCIDN: A reputation-based collaborative intrusion detection network to lessen the impact of malicious alarms. *Journal of network and systems management, 21*(1), 128-167.

Powers, D. M. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness & correlation. *Journal of Machine Learning Technologies, 2*(1), 37-63.

Rathore, M. M., Ahmad, A., & Paul, A. (2016). Real time intrusion detection system for ultra-high-speed big data environments. *The Journal of Supercomputing, 72*(9), 3489-3510.

RBS. (2019). The 2018 Year End Vulnerability QuickView Report - Risk Based Security. Retrieved Oct 18, 2019, from https://pages.riskbasedsecurity.com/2018-ye-vulnerability-quickview-report

Reddy, N. (2019a). Introduction to Cyber Forensics *Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations* (pp. 1-28). Berkeley, CA: Apress.

Reddy, N. (2019b). Web Attack Forensics *Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations* (pp. 317-344). Berkeley, CA: Apress.

Shah, S. A. R., & Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems, 80*, 157-170.

Shirey, R. (2007). RFC4949 - Internet Security Glossary, Version 2. Retrieved Sep 17, 2019, from https://tools.ietf.org/html/rfc4949

Shodan. (2019). EternalBlue vulnerabilities. Shodan. Retrieved Oct 16, 2019, from https://www.shodan.io/report/S8dhzrSn

Siris, V. A., & Papagalou, F. (2006). Application of anomaly detection algorithms for detecting SYN flooding attacks. *Computer communications, 29*(9), 1433-1442.

Stallings, W., & Brown, L. (2018). *Computer Security, Principles and Practice* (4 ed.): Pearson.

Symantec. (2019). Zero-day vulnerability: What it is, and how it works. Retrieved Oct 10, 2019, from https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

Thames, J. L. (2014). Distributed, Collaborative and Automated Cybersecurity Infrastructures for Cloud-Based Design and Manufacturing Systems. In D. Schaefer (Ed.), *Cloud-Based Design and Manufacturing (CBDM): A Service-Oriented Product Development Paradigm for the 21st Century* (pp. 207-229). Cham: Springer International Publishing.

Tucek, J., Newsome, J., Lu, S., Huang, C., Xanthos, S., Brumley, D., Zhou, Y., & Song, D. (2007). *Sweeper: A lightweight end-to-end system for defending against fast worms.* Paper presented at the ACM SIGOPS Operating Systems Review.

Van Steen, M., & Tanenbaum, A. S. (2017). *Distributed Systems* (3rd ed.): CreateSpace.

Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M., & Fischer, M. (2015). Taxonomy and Survey of Collaborative Intrusion Detection. *ACM Computing Surveys (CSUR), 47*(4), 55.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Wang, Y., Wen, S., Xiang, Y., & Zhou, W. (2013). Modeling the propagation of worms in networks: A survey. *IEEE Communications Surveys & Tutorials, 16*(2), 942-960.

Wang, Y., Xie, L., Li, W., Meng, W., & Li, J. (2017). *A Privacy-Preserving Framework for Collaborative Intrusion Detection Networks Through Fog Computing.* Paper presented at the Cyberspace Safety and Security, Cham.

Whittaker, Z. (2019). Two years after WannaCry, a million computers remain at risk. Retrieved Oct 16, 2019, from https://techcrunch.com/2019/05/12/wannacry-two-years-on/

Wilhelm, T., & Andress, J. (2011). Chapter 8 - Use of Timing to Enter an Area. In T. Wilhelm & J. Andress (Eds.), *Ninja Hacking* (pp. 119-134). Boston: Syngress.

Xie, Y., Sekar, V., Maltz, D. A., Reiter, M. K., & Zhang, H. (2005). *Worm origin identification using random moonwalks.* Paper presented at the 2005 IEEE Symposium on Security and Privacy (S&P'05).

Ye, N., Borror, C., & Zhang, Y. (2002). EWMA techniques for computer intrusion detection through anomalous changes in event intensity. *Quality and Reliability Engineering International, 18*(6), 443-451.

Yegneswaran, V., Barford, P., & Jha, S. (2004). *Global Intrusion Detection in the DOMINO Overlay System.* Paper presented at the NDSS.

Zhai, L., Guo, W., Jia, Z., Guo, L., & Shi, J. (2012). *Worm propagation model for heterogeneous network*.

Zhou, C. V., Karunasekera, S., & Leckie, C. (2005). *A peer-to-peer collaborative intrusion detection system*.

Zhou, C. V., Leckie, C., Karunasekera, S., & Peng, T. (2008). *A self-healing, self-protecting collaborative intrusion detection architecture to trace-back fast-flux phishing domains*.