**UNIVERSITI PUTRA MALAYSIA**

***CONTACT TRACING STRATEGY TO ISOLATE INFECTIOUS BOTS IN MITIGATING IOT BOTNET PROPAGATION AND PRESERVE OBJECT OF FORENSIC INTEREST***

**MOHAMMED IBRAHIM**

**FSKTM 2022 7**

# CONTACT TRACING STRATEGY TO ISOLATE INFECTIOUS BOTS IN MITIGATING IOT BOTNET PROPAGATION AND PRESERVE OBJECT OF FORENSIC INTEREST

By

**MOHAMMED IBRAHIM**

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

**June 2021**

**DEDICATION**

*To My Parent, Wife and My Children.*

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

**CONTACT TRACING STRATEGY TO ISOLATE INFECTIOUS BOTS IN MITIGATING IOT BOTNET PROPAGATION AND PRESERVE OBJECT OF FORENSIC INTEREST**

By

**MOHAMMED IBRAHIM**

**June 2021**

**Chairman: Professor Madya Mohd Taufik Abdullah, PhD**
**Faculty: Computer Science and Information Technology**

The emergence of Internet of Things (IoT) can facilitate and revolutionize various aspects of people's lives. However, most IoT devices are vulnerable to botnet attacks. To defend these devices against botnet attacks, first approach is to detect the transmission rate of the botnet infection based on the impact of network or bot's parameters. The second approach is to mitigate the size of the botnet infection by limiting the impact of the attack. The third approach is to ensures other nodes interacting with the existing bots are not infected. Notably, contact tracing strategy as an epidemic concept detects the impact of the infectious bots and isolates them from the network, thus minimizing the size of the botnet attack. Motivated by these, this thesis is aimed at overcoming three research gaps in line with defending IoT-WSN against botnet attack using contact tracing strategy.

In the abandon stage of the botnet life cycle, bots' memory efficiency affect the botmaster's decision to select or abandon the infectious bots for onward propagation of the attack. However, from the existing literature no work has actually studied the impact of memory-efficient bots on IoT botnet transmission rate. Hence, the first contribution in this thesis conceptualizes botmaster behavior with respect to the bots' memory availability. In this context, an abandoned class is introduced into the epidemic model by defining an abandon rate which prioritizes the memory-efficient bots during propagation. This model detects the impact of memory-efficient bots on the transmission rate of the botnet infection (which is generally unknown). Results from simulations show that the transmission rate of the botnet infection increases by 25.31% to 26.9% as the botmaster exploits the memory-efficient bots.

In the absence of an effective vaccine to mitigate malware propagation, contact tracing strategy is deployed to isolate the infectious nodes in order to minimize their impact on the attack. However, available literature shows that immunization and patching methods are predominantly used to limit the size of the IoT botnet infection. These methods are considered ineffective as the bots often update with new exploits that make the recovered devices vulnerable to the same attack. In this thesis, contact tracing strategy has been adopted in mitigating IoT botnet propagation such that infectious bots are transferred to the forensic class. To achieve this, an isolation parameter based on a sensor node sleeping rate transform the infectious bots into an inactive mode. Results obtained from simulations show that there is 25.67% decrease in the botnet infection peak value, 2 hours delay in the infection peak period and 33.33% delay in the propagation time.

Similarly, with the transfer of infectious bots to the forensic class, preserving these nodes remains a challenge due to autonomous interactions and packet collisions. Motivated by the concept of quarantine, the third contribution in this thesis quarantine the infectious bots by deriving a model that associates a safe-carrier sensing power threshold to the forensic class which minimizes packet collision. Consequently, the result shows that 66.67% of forensic nodes are preserved in the IoT platform.

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

**STRATEGI PENGESAN KONTAK UNTUK MENGASINGKAN BOT BERJANGKIT DALAM MENGURANGKAN PENYEBARAN BOTNET IOT DAN MEMELIHARA OBJEK KEPENTINGAN FORENSIK**

Oleh

**MOHAMMED IBRAHIM**

**Jun 2021**

**Pengerusi: Profesor Madya Mohd Taufik Abdullah, PhD**
**Fakulti: Sains Komputer dan Teknologi Maklumat**

Kemunculan Internet of Things (IoT) boleh memudahkan dan merevolusikan pelbagai aspek kehidupan manusia. Walau bagaimanapun, kebanyakan peranti IoT terdedah kepada serangan botnet. Untuk mempertahankan peranti ini daripada serangan botnet, pendekatan pertama adalah untuk mengesan kadar penghantaran jangkitan botnet berdasarkan kesan rangkaian atau parameter bot. Pendekatan kedua adalah untuk mengurangkan saiz jangkitan botnet dengan mengehadkan kesan serangan. Pendekatan ketiga adalah untuk memastikan nod lain yang berinteraksi dengan bot sedia ada tidak dijangkiti. Terutama, strategi pengesanan kenalan sebagai konsep wabak mengesan kesan bot berjangkit dan mengasingkannya daripada rangkaian, sekali gus meminimumkan saiz serangan botnet. Didorong oleh ini, tesis ini bertujuan untuk mengatasi tiga jurang penyelidikan selaras dengan mempertahankan IoT-WSN daripada serangan botnet menggunakan strategi pengesanan kenalan.

Dalam peringkat meninggalkan kitaran hayat botnet, kecekapan ingatan bot mempengaruhi keputusan botmaster untuk memilih atau meninggalkan bot berjangkit untuk penyebaran serangan seterusnya. Walau bagaimanapun, daripada kesusasteraan sedia ada tiada kerja yang benar-benar mengkaji kesan bot cekap memori pada kadar penghantaran botnet IoT. Oleh itu, sumbangan pertama dalam tesis ini mengkonsepkan tingkah laku botmaster berkenaan dengan ketersediaan memori bot. Dalam konteks ini, kelas terbengkalai diperkenalkan ke dalam model wabak dengan mentakrifkan kadar terbengkalai yang mengutamakan bot cekap ingatan semasa penyebaran. Model ini mengesan kesan bot cekap ingatan pada kadar penghantaran jangkitan botnet (yang umumnya tidak diketahui). Keputusan daripada simulasi menunjukkan bahawa kadar penghantaran jangkitan botnet meningkat sebanyak 25.31%

kepada 26.9% kerana botmaster mengeksploitasi bot yang cekap memori.

Sekiranya tiada vaksin yang berkesan untuk mengurangkan penyebaran perisian hasad, strategi pengesanan kenalan digunakan untuk mengasingkan nod berjangkit untuk meminimumkan kesannya terhadap serangan. Walau bagaimanapun, literatur yang ada menunjukkan bahawa kaedah imunisasi dan tampalan kebanyakannya digunakan untuk mengehadkan saiz jangkitan botnet IoT. Kaedah ini dianggap tidak berkesan kerana bot sering mengemas kini dengan eksploitasi baharu yang menjadikan peranti yang dipulihkan terdedah kepada serangan yang sama. Dalam tesis ini, strategi pengesanan kenalan telah diguna pakai dalam mengurangkan penyebaran botnet IoT supaya bot berjangkit dipindahkan ke kelas forensik. Untuk mencapai matlamat ini, parameter pengasingan berdasarkan kadar tidur nod sensor mengubah bot berjangkit kepada mod tidak aktif. Keputusan yang diperoleh daripada simulasi menunjukkan terdapat penurunan 25.67% dalam nilai puncak jangkitan botnet, 2 jam kelewatan dalam tempoh puncak jangkitan dan 33.33 % kelewatan dalam masa pembiakan.

Begitu juga, dengan pemindahan bot berjangkit ke kelas forensik, mengekalkan nod ini kekal sebagai cabaran kerana interaksi autonomi dan perlanggaran paket. Didorong oleh konsep kuarantin, sumbangan ketiga dalam tesis ini mengkuarantin bot berjangkit dengan menghasilkan model yang mengaitkan ambang kuasa penderiaan pembawa selamat kepada kelas forensik yang meminimumkan perlanggaran paket. Akibatnya, keputusan menunjukkan bahawa 66.67% daripada nod forensik dipelihara dalam platform IoT.

## ACKNOWLEDGEMENTS

I want to thank ALLAH for sparing my life and giving me the opportunity to upgrade my knowledge to being a Doctor of Philosophy candidate. I have experienced many things for which my knowledge has been broaden to a new horizon.

Archiving and completing task like this would have been impossible without the support and encouragement of many individuals. First, I would like to pay my respects and special thanks to my supervisor (Assoc. Prof. Dr. Mohd Taufik Abdullah) for his technical guides and constructive criticism which has significantly contributed to the success of this thesis. His academic and professional guide has been a great asset to have at the point of loss, and I sincerely appreciate that. My appreciation to Assoc. Prof. Dr. Azizol bin Abdullah and Assoc. Prof. Dr. Thinagaran Perumal for not only assisting me but guiding and providing pieces of advice and comments to accomplish this work. Also, acknowledge the great help and cooperation of the staff and students of University Putra Malaysia (UPM), most especially the Faculty of Computer Science and Information Technology and as well colleagues from Mathematics and Statistics departments for their cooperation.

Finally, I would like to thank the Management of Kaduna State University, and Tertiary Education Trust Fund under the Federal Government of Nigeria for sponsoring my study. Special thanks also to my parents, wife, children, brothers and sisters for their support, encouragement and understand during the period of this task.

Mohammed Ibrahim

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:

**Mohd Taufik Bin Abdullah, PhD**
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

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

**Thinagaran Perumal, 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 February 2022

**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: Associate Professor Dr. Mohd Taufik Abdullah

Signature: ______________________________
Name of
Member of
Supervisory
Committee: Associate Professor Dr. Azizol Abdullah

Signature: ______________________________
Name of
Member of
Supervisory
Committee: Dr. Thinagaran Perumal

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| IoT | Internet of Thing |
| WSN | Wireless Sensor Network |
| OOFF | Object of Forensic Interest |
| DDoS | Distributed Denial of Service |
| $R_0$ | Basic Reproduction Number |
| D2D | Device to Device |
| SIS | Susceptible Infectious Susceptible |
| SIR | Susceptible Infectious Recovered |
| TPWM | Topological Aware Worm Propagation |
| MAC | Medium Access Control |
| SID | Susceptible Infectious Dead |
| EiSIRS | Expanded improved Susceptible Infectious Recovered Susceptible |
| SIED | Susceptible Infectious Immune Dead |
| SEIRS-V | Susceptible Exposed Infectious Recovered Susceptible and Vaccination |
| SEIQRS-V | Susceptible Exposed Infectious Quarantine, Recovered and Vaccinated |
| SIRS | Susceptible Infectious Recovered Susceptible |
| SIQR | Susceptible Infectious Quarantine, Recovered |
| SIQRS | Susceptible Infectious Quarantine, Recovered, Susceptible |
| SEIRV | Susceptible Exposed Infectious, Recovered, Vaccination |
| C& C | Command and Control |
| LDS | Local Defending Strategy |
| SI | Susceptible-Infectious |

| | |
|---|---|
| IoT-SIA | IoT- Susceptible Infectious Abandon |
| IoT-SIAF | IoT- Susceptible Infectious Abandon, Forensic |
| IoT-SIAF-Q | IoT- Susceptible Infectious Abandon, Forensic, Quarantine |
| P2P | Peer-to-Peer |
| $P_{S(i,t)}$ | Probability of Susceptible State |
| $P_{C(i,t)}$ | Probability of Contagious State |
| $P_{I(i,t)}$ | Probability of Infectious State |
| IoT-BAI | IoT Botnet with Attack Information |
| ROM | Read Only Memory |
| SI/NS | Susceptible Infected/Non-Vulnerable-Susceptible |
| $S_{loc}$ | fraction of S in the local network |
| $S_{nhb}$ | fraction of S in the neighbor nodes |
| $\beta_R$ | Random Scanning based |
| $\beta_L$ | local Scanning based |
| $\beta_P$ | P2P based |
| $dth_B$ | death rate due to standard activities |
| $dth_R$ | death rate due to random scanning |
| $dth_L$ | death rate due to local scanning |
| $dth_P$ | death rate driving by P2P |
| $I_R$ | fraction of infected nodes via random scanning |
| $I_L$ | fraction of infected nodes via local scanning |
| $I_P$ | fraction of infected nodes via P2P scanning |

# CHAPTER 1

# INTRODUCTION

## 1.1 Background

The interconnection of embedded smart objects into the existing internet infrastructure have resulted in a new era of internet application known as "Internet of Things" or IoT. The term IoT was first coined by Kelvin Ashton in the year 1999 (Ashton et al., 2009). IoT application integrates different objects, sensors and intelligent devices to communicate autonomously without human intervention (Ambrosin et al., 2016). These intelligent devices are now deployed in a wide range of application that include but not limited to smart grid technology, healthcare and transport systems (Chifor et al., 2018). In addition, reliance of IoT devices on cloud infrastructure for storing, transfer and analysis of data led to the emergence of cloud-enabled IoT network (Mai and Khalil, 2017). However, the heterogeneity between various devices in IoT and diversity of application in its infrastructure posses the most tremendous challenge in its deployment. Besides, the increasing number of IoT devices has become a major cause of concern as several types of different malicious network (botnet) are been built by combining large scale of available IoT devices (Hoque et al., 2015). The goal and characteristics of each IoT botnet family is depicted in Table1.1 (Dzulqarnain, 2019)

**Table 1.1: IoT botnet family**

| Botnet Family | Goal | Characteristics |
|---|---|---|
| Bashlite | DDoS | Infecting an IoT device by brute forcing Telnet protocol using known default credentials |
| BrickerBot | DDoS | Brute-forcing Telnet credentials on ISPs leaving port 7547 |
| Hajime | Not known yet | Using several attack methods consist of, Telnet default password attack and vulnerability on ISP |
| New Aidra | DDoS | Brute-forcing IoT device via Telnet protocol |
| Mirai | DDoS | Brute-forcing devices via Telnet protocol and TCP/2323 |
| VPNFilter | Steal data | Specifically targeting router and NAS devices via 3 stage of infection |

Each IoT botnet family differs in characteristics that include several information such as their target, communication with controller and types of attack vector (Kumar and Lim, 2019). However, with the exception of Hajime and VPNFilter, other IoT botnet family are known with an established goal of Distributed Denial of Service attack (DDoS) attack. Lately, Mirai has deceived more than 600,000 devices to propagate itself in order to cause series of large-scale DDoS attacks across various countries around the globe with most of the attacks coming from South America and South-east Asia(Antonakakis et al., 2017). Countries like Brazil, Vietnam and Colombia appeared to constitute the most leading sources of infected devices as can be seen in Figure 1.1 (Bursztein, 2017).

Besides Mirai penetration capability around various geo-location of the globe, IoT malware is becoming increasingly adaptive and sophisticated with many recent features like IPv6 support, sophisticated communication methods between bots, and Command and Control (Angrishi, 2017). Since its first appearance in the past decades, the spread of malware has been accounting for a significant share of financial losses in the area of computer security (Data and Wang, 2005). Moreover, malware in an infected device might attempt to replicate itself in nearby devices (Farooq and Zhu, 2018). In the case of wireless IoT networks, the malware may spread among devices that are in close geographical proximity (Farooq and Zhu, 2018).

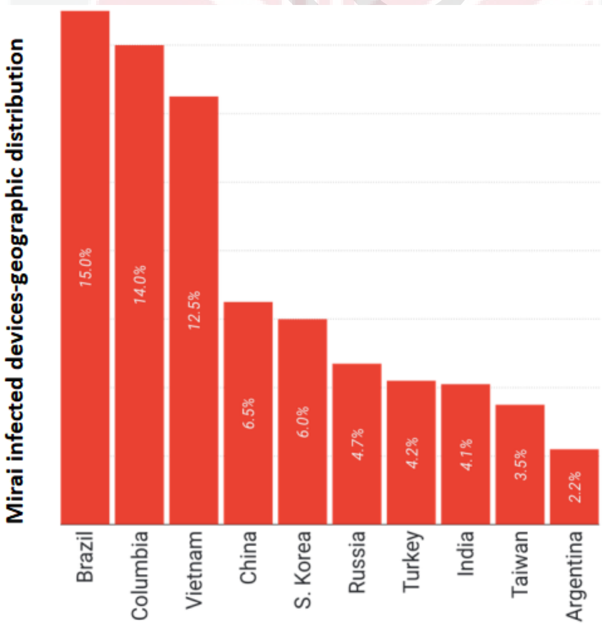


**Figure 1.1: Mirai Attack Geographical Distribution Chart**

However, such propagation is typically a challenging process to observe and detect due lack of experience of widespread implementation of new technologies that emerge across the globe with different vulnerabilities (Acarali et al., 2019). Hence different services or functions can serve as a propagation vector.

On the other hand, most IoT malware does not use reflection or amplification techniques to launch an attack, so it is much difficult to recognize and mitigate the attack using conventional methods (Angrishi, 2017). Consequently, some researchers used modeling approaches. Based on their understanding of the technology and experience of historic attacks to predict propagation dynamics in order to explore the influential factors (Acarali et al., 2019). Angrishi (2017) in their work recommend a non-technical approaches and policies in mitigating malware propagation and the impact of the attack thereafter. Primarily, the aim of mitigating IoT malware propagation is to reduce its propagation over the IoT network infrastructure. With the current trends, where IoT mitigation models relied on patching and immunization, bots often update themselves with new exploits that cannot be mitigated using patching and immunization. Potential application of IoT devices alongside their WSN background is trending across the globe. Without effective vaccines or treatment botnet attack with its propagation potentials can become one of the main threats to the security of the IoT network. It has become pertinent to mitigate the attack propagation in the absence of effective vaccine or treatment. To achieve this, infectious nodes are managed as an object of forensic interest that can be isolated for further forensic analysis.

## 1.2 Problem Statement

Mirai botnet is a worm-like family of malware that infected IoT devices and corralled them into a Distributed Denial of Service(DDoS) botnet (Antonakakis et al., 2017). To defend against IoT botnets attack, there is need for accurate understanding of its dynamic characteristics and its mode of propagation in a network. Although the recent study of Acarali et al. (2019) shows that Mirai botnet propagation mimics the dynamic of a typical worm propagation, in a worm propagation however, malicious program injects itself into the program memory of a sensor devices and self-propagate to other nodes (Giannetsos et al., 2009). On contrarily, in a Mirai botnet propagation, besides running the malicious program in the bots, existing bots execute the attacker's instruction and scan information about the target nodes as a necessary condition to propagate the attack (Ji et al., 2018). The mechanism employed by the Mirai botnet propagation is quite distinct from that of worm propagation. With Mirai botnet propagation, dynamics models of worm propagation cannot be used directly to analyze the dynamic of IoT botnet propagation.

However, the previous approaches of Ji et al. (2018), Acarali et al. (2019), Yin et al. (2019) and Xia et al. (2020) proposed dynamic IoT botnet propagation models for analyzing the size of the infection scale, base on IoT-WSN and social characteristics.

Common to these models, is that they only detect the size of the botnet transmission rate from the perspective of the initial number of bots in the network (Ji et al., 2018), bots' energy (Acarali et al., 2019) and devices' spreading capability (Xia et al., 2020) without due consideration to the botnet life cycle. Besides the execution of the attacker's instructions, in the botnet life cycle, the attacker runs malicious program in the bot memory and scan information about the target nodes for onward propagation of attack (Ji et al., 2018). With this in mind, the botnet life cycle cannot only affect the bots' processing capability but its ability to propagate the attack. Thus, memory-efficient bots can have aiding impact on the botnet propagation. Based on the knowledge from literature, no work has done on detecting or defending IoT network against memory-efficient bots. The impact of memory-efficient bots on the botnet transmission rate and the infection scale cannot be detected from the perspective of the botnet life Cycle. Consequently, investigating and mitigating the impact of botnet propagation will be difficult. In an effort to mitigate the impact of botnet and other IoT malware propagation, Jerkins and Stupiansky (2018) employed immunization and patches approach based on inoculation method to slow down the propagation rate and the infection peak value.

Nevertheless, devices recovered via patching are likely to be reinfected to the same malware attack since bots frequently receive update containing new exploits (Acarali, 2019). Hence, the recurring of infectious bots in the IoT network will increase the propagation rate. This instead result in minimizing few number of bots in the IoT network. However, in the absence of effective immunization, it will be paramount to isolate the infectious bots for forensic analysis.

Similarly, with the infectious bots isolated as object of forensic interest (OOFI), preservation of the scene is a contentious issue in digital forensic (Hegarty et al., 2014). This is due to the collision, real and autonomous interaction that might exist among the remaining nodes in the network. Even though hash value was employed by Rizal et al. (2018) to preserve the forensic data by protecting all evidence data, but according to Conti et al. (2018) preservation of scene is still a challenge in an IoT environment.Real-time and autonomous interactions between different nodes would make it very difficult if not impossible to identify the scope of compromise nodes and boundaries of a crime scene (Conti et al., 2018).

## 1.3 Research Questions

The research problems highlighted above raises the need to address the following questions:

- Does the memory-efficient bots have potential impact on the IoT botnet transmission rate?
- How does the isolation of the infectious bots into forensic class can reduce the botnet infection peak value and reduce the propagation rate of the botnet

attack?

- How to preserve the infectious nodes from autonomous interaction with different nodes and determine the scope of the scene in an IoT platform?

## 1.4 Research objectives

The main objective of this research is to propose contact-based tracing strategy model for modeling and analyzing the current issues in mitigating IoT botnet propagation. Similarly the proposed model will bridge the gap between the botnet epidemic emergency and the vaccine availability. To achieve this, the following objectives are considered:

- To propose a dynamic botnet propagation model for determining the botnet transmission rate with a view to detects the impact of memory-efficient bots on IoT botnet propagation.
- To propose an isolation model that can separate the infectious bots for forensic analysis with a view to minimize the propagation rate and the botnet Infection peak value.
- To formulate a quarantine model that can preserves the physical state of the infectious bots from the autonomous interaction with different IoT nodes with a view to preserve the scope of the crime scene.

## 1.5 Scope of the Research

This research focuses on the mitigation of IoT botnet propagation over an IoT-WSN and does not intend to cover the network and the cloud level of an IoT infrastructure. Particularly, this research is centered on Mirai botnet propagation. As such, emphasis will be given to IP cameras due to their high rate of vulnerability to Mirai attack.

## 1.6 Summary of Contributions

To meet the objectives of this research, the main contributions are as follows:

- Proposed a novel dynamic propagation model that detects the impact of memory-efficient bots on IoT botnet propagation while factors for determining the most infectious bots is ascertained.
- To bridge the gap between the botnet endemic emergency and the availability of effective vaccine, an isolation-based model has been proposed. This proposed model together with add-on forensic class will ensure that not only infectious nodes are identified but also mitigate the botnet infection peak value.

- Proposed a novel quarantine model that can minimize the interaction of forensic nodes with the remaining nodes in the network. As such the model will not only preserve the forensic nodes but determine the scope of the crime scene for the purpose of search and seizure.

## 1.7 Thesis Outline

The subsequent thesis chapters are structured as follows:

Chapter 2-*Literature Review*. The chapter 2 introduces worm and botnet propagation in a wireless IoT infrastructure. The concept of contact tracing based on epidemiology theories is discussed. Similarly, previous models on malware (worm and botnet) propagation and its mitigation in IoT-WSN are discussed in details.

Chapter 3-*Research Methodology*. Overview of the research problem and the steps applied in this research is presented. The research modeling parameters were identified. Steps necessary in determining the model stability concerning its basic reproductive number $R_0$ and equilibrium conditions are presented here. The chapter will also discuss the measurement used to evaluate the performance of the models.

Chapter 4-*Modeling and Formalization Techniques Based on Contact Tracing Strategy*. Detail on the proposed models for Mitigating IoT botnet propagation is presented.

Chapter 5-*Result and Discussion*. The outcomes of the numerical simulation results for the proposed models in IoT botnet propagation is discussed here.

Chapter 6-*Conclusion and Future Work*. Conclusion and summary of the proposed study is presented in this chapter and recommendations for future direction.

## REFERENCES


Abomhara, M. and Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, pages 65–88.

Acarali, D., Rajarajan, M., Komninos, N., and Zarpelão, B. B. (2019). Modelling the spread of botnet malware in iot-based wireless sensor networks. *Security and Communication Networks*, 2019:1–13.

Alhanahnah, M., Lin, Q., Yan, Q., Zhang, N., and Chen, Z. (2018). Efficient signature generation for classifying cross-architecture iot malware. In *2018 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE.

Allen, L. J., Brauer, F., Van den Driessche, P., and Wu, J. (2008). *Mathematical epidemiology*, volume 1945. Springer.

Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S. R., Rahmani, A. M., and Liljeberg, P. (2016). On the feasibility of attribute-based encryption on internet of things devices. *IEEE Micro*, 36(6):25–35.

Anderson, R. M., Anderson, B., and May, R. M. (1992). *Infectious diseases of humans: dynamics and control*. Oxford university press.

Angrishi, K. (2017). Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. *arXiv preprint arXiv:1702.03681*.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., et al. (2017). Understanding the mirai botnet. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pages 1093–1110.

Ashton, K. et al. (2009). That 'internet of things' thing. *RFID journal*, 22(7):97–114.

Awasthi, S., Kumar, N., and Srivastava, P. K. (2020). A study of epidemic approach for worm propagation in wireless sensor network. *Intelligent computing in engineering. Advances in intelligent systems and computing. Singapore: Springer*, pages 315–326.

Becker, N. G., Glass, K., Li, Z., and Aldis, G. K. (2005). Controlling emerging infectious diseases like sars. *Mathematical biosciences*, 193(2):205–221.

Binxing, F., Xiang, C., and Wei, W. (2011). Survey of botnets. *Journal of Computer Research and Development*, 48(8):1315.

Bouchaud, F., Grimaud, G., Vantroys, T., and Buret, P. (2019). Digital investigation of iot devices in the criminal scene. *JUCS-Journal of Universal Computer Science*, 25:1199.

Bursztein, E. (2017). Inside mirai the infamous iot botnet: A retrospective analysis. *Elie Bursztein's site. https://www. elie. net/blog/security/inside-mirai-theinfamous-iot-botnet-a-retrospective-analysis (accessed May 26, 2020)*.

Ceron, J. M., Steding-Jessen, K., Hoepers, C., Granville, L. Z., and Margi, C. B. (2019). Improving iot botnet investigation using an adaptive network layer. *Sensors*, 19(3):727.

Chifor, B.-C., Bica, I., Patriciu, V.-V., and Pop, F. (2018). A security authorization scheme for smart home internet of things devices. *Future Generation Computer Systems*, 86:740–749.

Chowdhury, S., Khanzadeh, M., Akula, R., Zhang, F., Zhang, S., Medal, H., Marufuzzaman, M., and Bian, L. (2017). Botnet detection using graph-based feature clustering. *Journal of Big Data*, 4(1):1–23.

Conti, M., Dehghantanha, A., Franke, K., and Watson, S. (2018). Internet of things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78(2):544–546.

Cozzi, E., Graziano, M., Fratantonio, Y., and Balzarotti, D. (2018). Understanding linux malware. In *2018 IEEE symposium on security and privacy (SP)*, pages 161–175. IEEE.

Dargie, W. and Poellabauer, C. (2010). *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons.

Data, S. and Wang, H. (2005). The effectiveness of vaccinations on the spread of email-borne computer viruses. In *Canadian Conference on Electrical and Computer Engineering, 2005.*, pages 219–223. IEEE.

De, P., Liu, Y., and Das, S. K. (2007). An epidemic theoretic framework for evaluating broadcast protocols in wireless sensor networks. In *2007 IEEE International Conference on Mobile Adhoc and Sensor Systems*, pages 1–9. IEEE.

Del Rey, Á. M., Batista, F., and Dios, A. Q. (2017). Malware propagation in wireless sensor networks: global models vs individual-based models. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, 6(3):5–15.

Dibrov, Y. (2017). The internet of things is going to change everything about cybersecurity. *Harvard Business Review*.

Divita, J. and Hallman, R. A. (2017). An approach to botnet malware detection using nonparametric bayesian methods. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pages 1–9.

Dzulqarnain, D. (2019). Investigating iot malware characteristics to improve network security. Master's thesis, University of Twente.

Eberly, D. (2008). Stability analysis for systems of differential equations. *Geometric Tools, LLC*.

Enright, J. and Kao, R. R. (2018). Epidemics on dynamic networks. *Epidemics*, 24:88–97.

Eslahi, M., Salleh, R., and Anuar, N. B. (2012). Bots and botnets: An overview of characteristics, detection and challenges. In *2012 IEEE International Conference on Control System, Computing and Engineering*, pages 349–354. IEEE.

Farooq, M. J. and Zhu, Q. (2018). Modeling, analysis, and mitigation of dynamic botnet formation in wireless iot networks. *IEEE Transactions on Information Forensics and Security*, 14(9):2412–2426.

Feily, M., Shahrestani, A., and Ramadass, S. (2009). A survey of botnet and botnet detection. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, pages 268–273. IEEE.

Feng, L., Song, L., Zhao, Q., and Wang, H. (2015). Modeling and stability analysis of worm propagation in wireless sensor network. *Mathematical Problems in Engineering*, 2015:1–8.

Fu, L., Liew, S. C., and Huang, J. (2012). Effective carrier sensing in csma networks under cumulative interference. *IEEE Transactions on Mobile Computing*, 12(4):748–760.

Gandotra, E., Bansal, D., and Sofat, S. (2014). Malware analysis and classification: A survey. *Journal of Information Security*, 2014(5):56–64.

Gardner, M. T., Beard, C., and Medhi, D. (2017). Using seirs epidemic models for iot botnets attacks. In *DRCN 2017-Design of Reliable Communication Networks; 13th International Conference*, pages 1–8. VDE.

Giannetsos, T., Dimitriou, T., and Prasad, N. R. (2009). Self-propagating worms in wireless sensor networks acm conext-student workshop. pages 31–32.

Godrej (2020). Godrej cctv system faq. [Online; accessed 1-December-2020].

Govil, J. (2007). Examining the criminology of bot zoo. In *2007 6th International Conference on Information, Communications & Signal Processing*, pages 1–6. IEEE.

Guo, W., Zhai, L., Guo, L., and Shi, J. (2012). Worm propagation control based on spatial correlation in wireless sensor network. In *Asia-Pacific Web Conference*, pages 68–77. Springer.

Hachem, N., Mustapha, Y. B., Granadillo, G. G., and Debar, H. (2011). Botnets: lifecycle and taxonomy. In *2011 Conference on Network and Information Systems Security*, pages 1–8. IEEE.

Haghighi, M. S., Wen, S., Xiang, Y., Quinn, B., and Zhou, W. (2016). On the race of worms and patches: Modeling the spread of information in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 11(12):2854–2865.

Hayel, Y. and Zhu, Q. (2017). Epidemic protection over heterogeneous networks using evolutionary poisson games. *IEEE Transactions on Information Forensics and Security*, 12(8):1786–1800.

Heffernan, J. M., Smith, R. J., and Wahl, L. M. (2005). Perspectives on the basic reproductive ratio. *Journal of the Royal Society Interface*, 2(4):281–293.

Hegarty, R., Lamb, D. J., and Attwood, A. (2014). Digital evidence challenges in the internet of things. In *INC*, pages 163–172.

Hejazi, P. and Ferrari, G. (2018). Energy and memory efficient data loss prevention in wireless sensor networks. *Preprints*, pages 1–18.

Hoang, X. D. and Nguyen, Q. C. (2018). Botnet detection based on machine learning techniques using dns query data. *Future Internet*, 10(5):43.

Honovich, J. (2009). Security manager's guide to video surveillance. *V3. IPVideo-Market. info.[online, ebook] Available: http://ipvideomarket. info/book*.

Hoque, N., Bhattacharyya, D. K., and Kalita, J. K. (2015). Botnet in ddos attacks: trends and challenges. *IEEE Communications Surveys & Tutorials*, 17(4):2242–2270.

Hossain, M., Karim, Y., and Hasan, R. (2018). Fif-iot: A forensic investigation framework for iot using a public digital ledger. In *2018 IEEE International Congress on Internet of Things (ICIOT)*, pages 33–40. IEEE.

Hu, Y.-C., Perrig, A., and Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. In *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)*, volume 3, pages 1976–1986. IEEE.

Jerkins, J. A. and Stupiansky, J. (2018). Mitigating iot insecurity with inoculation epidemics. In *Proceedings of the ACMSE 2018 Conference*, page 4. ACM.

Ji, Y., Yao, L., Liu, S., Yao, H., Ye, Q., and Wang, R. (2018). The study on the botnet and its prevention policies in the internet of things. In *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))*, pages 837–842. IEEE.

Jones, J. H. (2007). Notes on r0. *Califonia: Department of Anthropological Sciences*, pages 1–19.

Kamal, A. R. M., Bleakley, C. J., and Dobson, S. (2014). Failure detection in wireless sensor networks: A sequence-based dynamic approach. *ACM Transactions on Sensor Networks (TOSN)*, 10(2):1–29.

Kechen, Z., Hong, Z., and Kun, Z. (2012). Simulation-based analysis of worm propagation in wireless sensor networks. In *2012 Fourth International Conference on Multimedia Information Networking and Security*, pages 847–851. IEEE.

Kephart, J. O. and White, S. R. (1993). Measuring and modeling computer virus prevalence. In *Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 2–15. IEEE.

Khanh, N. H. (2016). Dynamics of a worm propagation model with quarantine in wireless sensor networks. *Appl. Math. Inf. Sci*, 10(5):1739–1746.

Khayam, S. A. and Radha, H. (2005). A topologically-aware worm propagation model for wireless sensor networks. In *25th IEEE international conference on distributed computing systems workshops*, pages 210–216. IEEE.

Khoshhalpour, E. and Shahriari, H. R. (2018). Botrevealer: Behavioral detection of botnets based on botnet life-cycle. *The ISC International Journal of Information Security*, 10(1):55–61.

Khosroshahy, M., Ali, M. K. M., and Qiu, D. (2013). The sic botnet lifecycle model: a step beyond traditional epidemiological models. *Computer Networks*, 57(2):404–421.

Ko, Y. M. and Gautam, N. (2010). Epidemic-based information dissemination in wireless mobile sensor networks. *IEEE/ACM Transactions on Networking*, 18(6):1738–1751.

Kok, J. and Kurz, B. (2011). Analysis of the botnet ecosystem. In *10th Conference of Telecommunication, Media and Internet Techno-Economics (CTTE)*, pages 1–10. VDE.

Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84.

Kumar, A. and Lim, T. J. (2019). Edima: early detection of iot malware network activity using machine learning techniques. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pages 289–294. IEEE.

Kwok, K. O., Tang, A., Wei, V. W., Park, W. H., Yeoh, E. K., and Riley, S. (2019). Epidemic models of contact tracing: Systematic review of transmission studies of severe acute respiratory syndrome and middle east respiratory syndrome. *Computational and structural biotechnology journal*, pages 186–194.

Kyrychko, Y. N. and Blyuss, K. B. (2005). Global properties of a delayed sir model with temporary immunity and nonlinear incidence rate. *Nonlinear analysis: real world applications*, 6(3):495–507.

Lei, C., Bie, H., Fang, G., Gaura, E., Brusey, J., Zhang, X., and Dutkiewicz, E. (2016). A low collision and high throughput data collection mechanism for large-scale super dense wireless sensor networks. *Sensors*, 16(7):1108.

Li, Z. and Liao, Q. (2014). Toward a monopoly botnet market. *Information Security Journal: A Global Perspective*, 23(4-6):159–171.

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., and Zhang, J. (2009). Botnet: classification, attacks, detection, tracing, and preventive measures. *EURASIP journal on wireless communications and networking*, 2009:1–11.

Lu, C. and Brooks, R. (2011). Botnet traffic detection using hidden markov models. In *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, pages 1–1.

Lu, Z., Wang, W., and Wang, C. (2015). On the evolution and impact of mobile botnets in wireless networks. *IEEE Transactions on Mobile Computing*, 15(9):2304–2316.

Mai, V. and Khalil, I. (2017). Design and implementation of a secure cloud-based billing model for smart meters as an internet of things using homomorphic cryptography. *Future Generation Computer Systems*, 72:327–338.

Mathur, K. and Hiranwal, S. (2013). A survey on techniques in detection and analyzing malware executables. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(4):422–428.

Mishra, B. K. and Keshri, N. (2013). Mathematical model on the transmission of worms in wireless sensor network. *Applied Mathematical Modelling*, 37(6):4103–4111.

Mishra, B. K. and Tyagi, I. (2014). Defending against malicious threats in wireless sensor network: A mathematical model. *International Journal of Information Technology and Computer Science*, 6(3):12–19.

Ojha, R. P., Sanyal, G., Srivastava, P. K., and Sharma, K. (2017). Design and analysis of modified siqrs model for performance study of wireless sensor network. *Scalable Computing: Practice and Experience*, 18(3):229–242.

Osanaiye, O., Alfa, A. S., and Hancke, G. P. (2018). A statistical approach to detect jamming attacks in wireless sensor networks. *Sensors*, 18(6):1691.

Peak, C. M., Childs, L. M., Grad, Y. H., and Buckee, C. O. (2017). Comparing nonpharmaceutical interventions for containing emerging epidemics. *Proceedings of the National Academy of Sciences*, 114(15):4023–4028.

Posny, D. and Wang, J. (2014). Computing the basic reproductive numbers for epidemiological models in nonhomogeneous environments. *Applied Mathematics and Computation*, 242:473–490.

Qiu, T., Liu, J., Si, W., and Wu, D. O. (2019). Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks. *IEEE/ACM Transactions on Networking*, 27(3):1028–1042.

Ren, J., Yang, X., Yang, L.-X., Xu, Y., and Yang, F. (2012). A delayed computer virus propagation model and its dynamics. *Chaos, Solitons & Fractals*, 45(1):74–79.

Rizal, R., Riadi, I., and Prayudi, Y. (2018). Network forensics for detecting flooding attack on internet of things (iot) device. *Int. J. Cyber-Secur. Dig. Forensics (IJCSDF)*, 7:382–390.

Rohbanian, M. R., Kharazmi, M. R., Keshavarz-Haddad, A., and Keshtgary, M. (2013). Watchdog-leach: a new method based on leach protocol to secure clustered wireless sensor networks. *arXiv preprint arXiv:1310.3637*, pages 1–12.

SCW (2018). Installation instructions for 32 channel admiral systems and 32-128 channel imperial systems. [Online; accessed 17-December-2020].

Servida, F. and Casey, E. (2019). Iot forensic challenges and opportunities for digital traces. *Digital Investigation*, 28:S22–S29.

Shen, S., Li, H., Han, R., Vasilakos, A. V., Wang, Y., and Cao, Q. (2014). Differential game-based strategies for preventing malware propagation in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 9(11):1962–1973.

Singh, A., Awasthi, A. K., Singh, K., and Srivastava, P. K. (2018). Modeling and analysis of worm propagation in wireless sensor networks. *Wireless Personal Communications*, 98(3):2535–2551.

Soetaert, K., Petzoldt, T., and Setzer, R. (2016). desolve: Solvers for initial value problems of differential equations (ode, dae, dde). *R package version*, 1.

Song, L.-P., Jin, Z., and Sun, G.-Q. (2011). Modeling and analyzing of botnet interactions. *Physica A: Statistical Mechanics and its Applications*, 390(2):347–358.

Sun, B., Yan, G., Xiao, Y., and Yang, T. A. (2008). Self-propagating mal-packets in wireless sensor networks: Dynamics and defense implications. *Ad Hoc Networks*, 7(8):1489–1500.

Tang, S. and Mark, B. L. (2009). Analysis of virus spread in wireless sensor networks: An epidemic model. In *2009 7th International Workshop on Design of Reliable Communication Networks*, pages 86–91. IEEE.

Wainwright, P. and Kettani, H. (2019). An analysis of botnet models. In *Proceedings of the 2019 3rd International Conference on Compute and Data Analysis*, pages 116–121.

Wang, T., Wu, Q., Wen, S., Cai, Y., Tian, H., Chen, Y., and Wang, B. (2017). Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks. *Sensors*, 17(1):139.

Wang, X., Li, Q., and Li, Y. (2010). Eisirs: a formal model to analyze the dynamics of worm propagation in wireless sensor networks. *Journal of Combinatorial Optimization*, 20(1):47–62.

Wei, S. and Chen, J. (2009). Modeling the spread of worm epidemics in wireless sensor networks. In *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4. IEEE.

Winward, R. (2018). Iot attack handbook: A field guide to understanding iot attacks from the mirai botnet and its modern variants. In *Security Evangelist, Radware*, pages 1–46. Security Evangelist, Radware.

Xia, H., Li, L., Cheng, X., Cheng, X., and Qiu, T. (2020). Modeling and analysis botnet propagation in social internet of things. *IEEE Internet of Things Journal*, 7(8):7470–7481.

Xia, H., Xiao, F., Zhang, S.-s., Hu, C.-q., and Cheng, X.-z. (2019). Trustworthiness inference framework in the social internet of things: A context-aware approach. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 838–846. IEEE.

Yin, M., Chen, X., Wang, Q., Wang, W., and Wang, Y. (2019). Dynamics on hybrid complex network: Botnet modeling and analysis of medical iot. *Security and Communication Networks*, 2019.

Yu, S., Wang, G., and Zhou, W. (2015). Modeling malicious activities in cyber space. *IEEE network*, 29(6):83–87.

Zema, N. R., Natalizio, E., Poss, M., Ruggeri, G., and Molinaro, A. (2014). Healing wireless sensor networks from malicious epidemic diffusion. In *2014 IEEE International Conference on Distributed Computing in Sensor Systems*, pages 171–178. IEEE.

Zhang, Z., Kundu, S., and Wei, R. (2019). A delayed epidemic model for propagation of malicious codes in wireless sensor network. *Mathematics*, 7(5):396.

Zhao, D., Wang, L., Wang, Z., and Xiao, G. (2018). Virus propagation and patch distribution in multiplex networks: modeling, analysis, and optimal allocation. *IEEE Transactions on Information Forensics and Security*, 14(7):1755–1767.

Zheng, X., Cai, Z., and Li, Y. (2018). Data linkage in smart internet of things systems: a consideration from a privacy perspective. *IEEE Communications Magazine*, 56(9):55–61.

# BIODATA OF STUDENT

The student, Mohammed Ibrahim, received B.Tech in Mathematics and Computer Science from Federal University of Technology, Minna, Nigeria in 2008, and his M.Sc in Security in Computing from Universiti Putra Malaysia (UPM) in 2014. He is currently a PhD candidate at the faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). His research interests includes digital forensic, Cyber Security, Smart system technology, and mitigation of malware propagation.

## LIST OF PUBLICATIONS

The following are the list of publications that arise from this study.

Mohammed Ibrahim, Mohd Taufik Abdullah, Azizol Abdullah, Thinagaran Perumal (2021). Correction To: The Impact of Memory-Efficient Bots on IoT-WSN Botnet Propagation. *Wireless Personal Communication.*, *doi: 10.1007/511277-021-08320-7*.

Mohammed Ibrahim, Muhammed Bashir Jasser, Mohd Taufik Abdullah, Azizol Abdullah (2019). Formalization in Digital Forensic Triage for Identification of Malicious IoT Devices. *Int. Journal of Engineering and Advanced Technology (IJEAT)*, Vol 9(1), *DOI:10.35940/ijeat.A2638.109119*.

Mohammed Ibrahim, Mohd Taufik Abdullah, Azizol Abdullah, Thinagaran Perumal (2020). An Epidemic Based Model for the prediction of OOFI in an IoT Platform. *Int. Journal of Engineering Trends and Technology (IJETT)*, *doi: 10.14445/22315381/CATI2P208*. ISSN:2231-5381

Mohammed Ibrahim, Mohd Taufik Abdullah, Azizol Abdullah, Thinagaran Perumal (2021). IoTContact: A Strategy For Predicting Contagious IoT Nodes In Mitigating Ransomware Attacks. *Turkish Journal of Computer and Mathematics Education*, Vol. 12(3)