Impact of Mobile Botnet on Long Term Evolution Networks: A Distributed Denial of Service Attack Perspective

by

Asem Kitana
B.Sc. of Computer Information Systems, Amman University, Jordan, 2005
M.Sc. of Networks Security, DePaul University, USA, 2007

A Dissertation Submitted in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Electrical and Computer Engineering

Impact of Mobile Botnet on Long Term Evolution Networks: A Distributed Denial of Service Attack Perspective

by

Asem Kitana
B.Sc. of Computer Information Systems, Amman University, Jordan, 2005
M.Sc. of Networks Security, DePaul University, USA, 2007

Supervisory Committee

Dr. Issa Traore, Co-Supervisor
(Department of Electrical and Computer Engineering, University of Victoria)

Dr. Isaac Woungang, Co-Supervisor
(Department of Computer Science, Ryerson University, Toronto, ON, Canada)

Dr. Kin Li, Departmental Member
(Department of Electrical and Computer Engineering, University of Victoria)

Dr. Alex Thomo, Outside Member
(Department of Computer Science, University of Victoria)

ABSTRACT

In recent years, the advent of Long Term Evolution (LTE) technology as a prominent component of 4G networks and future 5G networks, has paved the way for fast and new mobile web access and application services. With these advantages come some security concerns in terms of attacks that can be launched on such networks. This thesis focuses on the impact of the mobile botnet on LTE networks by implementing a mobile botnet architecture that initiates a Distributed Denial of Service (DDoS) attack. First, in the quest of understanding the mobile botnet behavior, a correlation between the mobile botnet impact and different mobile device mobility models, is established, leading to the study of the impact of the random patterns versus the uniform patterns of movements on the mobile botnet's behavior under a DDoS attack. Second, the impact of two base transceiver station selection mechanisms on a mobile botnet behavior launching a DDoS attack on a LTE network is studied, the goal being to derive the effect of the attack severity of the mobile botnet. Third, an epidemic SMS-based cellular botnet that uses an epidemic command and control mechanism to initiate a short message services (SMS) phishing attack, is proposed and its threat impact is studied and simulated using three random graphs models. The simulation results obtained reveal that (1) in terms of users' mobility patterns, the impact of the mobile botnet behavior under a DDoS attack on a victim web server is more pronounced when an asymmetric mobility model is considered compared to a symmetric mobility model; (2) in terms of base transceiver station selection mechanisms, the Distance-Based Model mechanism yields a higher threat impact on the victim server compared to the Signal Power Based Model mechanism; and (3) under the Erdos-and-Reyni Topology, the proposed epidemic SMS-based cellular botnet is shown to be resistant and resilient to random and selective cellular device failures.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

LTE Long Term Evolution

C&C Command and Control

4G Fourth Generation

DDoS Distributed Denial of Service

AMM Asymmetric Mobility Model

SMM Symmetric Mobility Model

DBM Distance-Based Model

SPBM Signal Power Based Model

eNodeB Evolved Node B

eNB eNodeB

SMS Short Message Service

BAT Barabasi–and-Albert Topology

ERT Erdos-and-Reyni Topology

WST Watts-and-Strogatz Topology

RWP Random Way-Point

1G First Generation

2G Second Generation

3G Third Generation

GSM Global System for Mobile

GPRS General Packet Radio Service

EDGE Enhanced Data rates for GSM Evolution

UMTS Universal Mobile Telecommunications System

HSPA High Speed Packet Access

3GPP Third Generation Partnership Project

P2P Peer-to-Peer

DoS Denial of Service

HLR Home Location Register

PAM Preferential Attachment Model

URL Uniform Resource Locator

ACD Average Cdevice Degree

CBS Cellular Botnet Size

EPS Evolved Packet System

EPC Evolved Packet Core

E-UTRAN Evolved UMTS Terrestrial Radio Access Network

UE User Equipment

HSS Home Subscriber Server

MME Mobility Management Entity

PGW Packet Data Network Gateway

SGW Serving Gateway

PDN Packet Data Network

APN Access Point Name

NAS Non-Access Stratum

AS Access Stratum

ESM EPS Session Management

EMM EPS Mobility Management

TDD Time Division Duplex

FDD Frequency Division Duplex

GTP GPRS Tunnelling Protocol

QoS Quality of Service

QCI QoS Class Identifier

GBR Guaranteed Bit Rate

IP Internet Protocol

IMS IP Multimedia Subsystem

FTP File Transfer Protocol

HTTP Hypertext Transfer Protocol

MAC Medium Access Control

RLC Radio Link Control

UDP User Datagram Protocol

TCP Transmission Control Protocol

HPLMN Home Public Land Mobile Network

RSRP Reference Signal Received Power

OFDM Orthogonal Frequency Division Multiplexing

NRB Number of Resource Blocks

GPS Global Positioning System

IMSI International Mobile Subscriber Identity

RRC Radio Resource Control

ARP Allocation and Retention Priority

BTS Base Transceiver Station

MTP Maximum Transmission Power

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisors Prof. Issa Traore, and Prof. Isaac Woungang for their continuous support of my Ph.D. study, their patience, motivation, and immense knowledge. Their guidance helped me in all the time of research and writing of this dissertation. It was a great privilege and honor to work under their guidance. I am extremely grateful for what they have offered me.

Their words of encouragement, guidance, and advice kept me active while achieving my research milestones. I just wanted to express how glad I am to work under their supervision. I am, truly, proud to be one of their students. Thank you, Prof. Traore and Prof. Woungang for everything.

My sincere thanks also go to Prof. Kin Li, and Prof. Alex Thomo, who accepted my request to join the Ph.D. dissertation committee, for their precious time, and for being members of the advisory team.

Also, I would like to thank my research group fellows, Dr. Sherif Saad, and Dr. Marcelo Brocardo for all the support they provided to me.

DEDICATION

I dedicate this work to my mother (in memory) and my father who always encouraged me to pursue my graduate studies.

Chapter 1

Introduction

1.1 Context

The evolving transformation of mobile networks technologies has led to the advent of the fourth generation (4G) networks, where superior services and applications, much higher speed, and low latency, are achieved. In the 4G architecture, the Long Term Evolution (LTE) standard represents the wireless mobile technology, which has multiple benefits, such as seamless integration with other non-LTE technologies, full interworking with heterogeneous networks (HetNets), and interoperability with different cellular base station technologies (e.g. Picocells and Femtocells). With the introduction of the Internet Protocol (IP)-based full interworking in LTE, the attack-surface has largely increased despite strong encryption and authentication [1]. Therefore, focusing on the security threat landscape in 4G networks, there is a clear demand for novel contributions that can enhance the resiliency and security of the LTE technology against various types of cyber-attacks launched against the network infrastructure.

Among these attacks are the DoS attacks on the Infrastructure. A DoS or Distributed DoS (DDoS) attack is usually launched to undermine the operation of critical infrastructure such as health, energy, telecommunication networks, transportation systems, to name a few. This type of attacks is often designed to exhaust the resources (both physical and logical) of the

targeted devices/system; and it is even more severe when issued from a large number of geographically dispersed machines. Focusing on this latter point, with the dominance of LTE networks and the accretion of mobile malware, LTE-based mobile botnets that initiate DDoS attacks has become greater in size, intensity, and sophistication. As a result, the attackers are lured to exploit and leverage the power of mobile devices (as the nodes of a LTE network) to establish mobile botnets that can effectively initiate DDoS attacks against various targets. This thesis studies the impact of LTE-based mobile botnet that initiates a DDoS attack against targeted systems, by designing, assessing, evaluating and validating a mobile botnet architecture over a LTE network.

1.2 Problem Statement

In the quest of understanding the mobile botnet behavior, and based on that architecture, in this thesis, a botnet architecture is designed, and based on it, the impact of the mobile botnet on LTE networks from three perspectives are investigated, namely: (1) the impact of the random patterns versus the uniform patterns on a mobile botnet, (2) the impact of base transceiver station selection mechanisms on a mobile botnet, and (3) the design of an epidemic SMS-based cellular botnet that uses an epidemic command and control mechanism.

As a matter of fact, the study of LTE-based mobile botnets is a new research domain which involves a number of key research challenges including the following:

- Unlike traditional botnets which rely on stationary devices (i.e. static devices) such as servers, LTE-based mobile botnets rely on mobile devices (i.e. portable devices). As a result, LTE-based mobile botnets have the distinctive feature of devices' mobility, that make the malicious impact of LTE-based mobile botnets relies on the human mobility. Therefore, the relationship between devices' mobility and the malicious operations of LTE-based mobile botnets should be investigated and evaluated, to find

suitable mechanisms that reduce and prevent the severity of such threat.

- A LTE-based mobile botnet acts as an overlay network that operates over the LTE infrastructure network. Thus, the Overlay-Infrastructure relationship plays a key role in the construction, operations, and impacts of LTE-based mobile botnets. In other words, the process of modifying some features, attributes, or characteristics of the LTE cellular network (the infrastructure network) should affect the LTE-based mobile botnet (the overlay network) operations. Consequently, this Overlay-Infrastructure relationship should be studied to reveal the characteristics of LTE network that most affect the impact of LTE-based mobile botnets.

- LTE-based mobile botnets are based on mobile devices, which by their nature have low storage, restricted processing power, and limited energy. As a result, LTE-based mobile botnets could lose their efficiency if the utilization of mobile devices lasts for long time. Therefore, the malicious operations of LTE-based mobile botnets should be run in short time and quickly to avoid any deficiency in their performance.

- Mobile devices could face hardware, software, or battery problems that could lead to losing the communication capabilities, halt, or shutdown in these mobile devices. Thus, effectual LTE-based mobile botnets should be resilient against the failure of mobile devices to guarantee the continuity of their malicious operations.

- Mobile devices support multiple services such as SMS service that relies on the functionality of cellular networks. As a result, all the SMS messages that will be sent between two ends over a LTE cellular network will be monitored. In addition, the process of sending SMS messages costs money. Therefore, forwarding too many SMS messages will draw the attention of cellular network operators and end users. Hence, LTE-based mobile botnets should be designed in a stealthy manner to avoid simple detection and mitigation techniques.

- Due to privacy concerns, the limited amount of resources on LTE-based mobile botnets, and the lack of examples and datasets on LTE-based mobile botnets contribute to the difficulty of studying LTE-based mobile botnets' operations and impact.

1.3 Approach

To address some of the above-mentioned challenges, LTE-based mobile botnets should be designed by employing three essential aspects, namely, rapid malware propagation, stealthy malware propagation, and resiliency to cellular devices' failure. In this thesis, the characteristics of a mobile botnet epidemic behavior are identified, and based on these, the elasticity of the mobile botnets is tested under different cellular devices failure scenarios. Also, the relationship between different mobility models, the severity level of mobile botnet attacks, and the relationship between different infrastructure cellular networks' attributes and the risk levels that are initiated by the mobile botnet attacks are investigated.

In order to understand the behavior of a mobile botnet, we have designed a botnet over a simulated LTE network and used real traces of taxi trajectory files to simulate the mobility patterns of mobile devices (i.e. Asymmetric Mobility Model (AMM) vs. Symmetric Mobility Model (SMM)), and study their impact on the mobile botnet behavior, showing that the SMM model reduces the impact of the DDoS attack on a victim server. Moreover, we have investigated the impact of two base transceiver station selection mechanisms, namely, the distance-based eNodeB (DBM) and the signal power-based eNodeB (SPBM) mechanisms, on a mobile botnet launching a DDoS attack on LTE network. The results reveal that in comparison to DBM, using SPBM to enable the mobile devices' connections with the serving eNodeB stations can reduce the impact of the attack severity level of the mobile botnet on the victim servers.

We have also studied the efficiency of mobile botnet behavior, measured in terms of epidemicity (i.e. speed and stealth characteristics) by deploying a SMS-based cellular botnet

that initiates a short message services (SMS) phishing attack. In doing this, an epidemic command and control mechanism is designed which is based on a flooding algorithm and three random graphs models are implemented as topologies for the mobile botnet operations, namely, the Barabasi–and-Albert topology (BAT), Erdos-and-Reyni topology (ERT), and Watts-and-Strogatz topology (WST), under two cellular devices failures, namely, random failure and selective failure; the goal being to measure the resistance and resilience of the designed mobile botnet. The results show that ERT is the best topology for enhancing the epidemic behavior of the proposed cellular botnet. The outcome of this research can serve as a basis for developing mobile botnet mitigation techniques.

1.4 Thesis Contributions

The contributions of this thesis are as follows:

- Implementation of a LTE-based mobile botnet architecture that initiates a DDoS attack and the study of the impact of mobility models on a LTE-based mobile botnet using this architecture.
- Study of the impact of Base Transceiver Station Selection Mechanisms on a mobile botnet over a LTE Network.
- Design of an epidemic SMS-based cellular botnet that uses an epidemic command and control mechanism against SMS phishing attacks on cellular networks and the study of its epidemic behavior using three well-known random graphs models.

1.4.1 Linkage of Scientific Papers

The proposed implementation of a LTE-based mobile botnet architecture that initiates a DDoS attack and the study of the impact of mobility models on a LTE-based mobile botnet using this architecture (i.e., Contribution 1) was published in Paper 1 (listed in subsection

1.4.2). Paper 1 (Impact Study of a Mobile Botnet over LTE Networks) studies the impact of the random patterns of movements' behavior (i.e. Asymmetric Mobility Model (AMM)) and the uniform patterns of movements' behavior (i.e. Symmetric Mobility Model (SMM)) on a LTE-based mobile botnet that initiates a DDoS attack.

The proposed deployment of a mobile botnet architecture that initiates a DDoS attack over a LTE network and the study of the impact of Base Transceiver Station Selection Mechanisms on such architecture (i.e., Contribution 2) was published in Paper 2 (listed in subsection 1.4.2). Paper 2 (Impact of Base Transceiver Station Selection Mechanisms on a Mobile Botnet over a LTE Network) investigates the impact of two base transceiver station selection mechanisms, namely, the distance-based eNodeB (DBM) and the signal power-based eNodeB (SPBM) mechanisms, on a mobile botnet launching a distributed denial of service (DDoS) attack over a Long Term Evolution (LTE) network.

The proposed design of an epidemic SMS-based cellular botnet that uses an epidemic command and control mechanism against SMS phishing attacks on cellular networks and the study of its epidemic behavior using three well-known random graphs models (i.e., Contribution 3) was published in Paper 3 (listed in subsection 1.4.2). Paper 3 (Towards an Epidemic SMS-based Cellular Botnet) proposes the design of an epidemic cellular botnet that initiates a SMS phishing attack by employing an epidemic command and control mechanism and studies its epidemic behavior using three random graphs models, namely the Barabasi–and-Albert topology (BAT), Erdos-and-Reyni topology (ERT), and Watts-and-Strogatz topology (WST).

1.4.2 List of Publications

[1] Asem Kitana, Issa Traore, and Isaac Woungang. Impact Study of a Mobile Botnet over LTE Networks. Journal of Internet Services and Information Security (JISIS), Volume 6, Number 2, Pages 1–22, May 2016.

[2] Asem Kitana, Issa Traore, and Isaac Woungang. Impact of Base Transceiver Station Selection Mechanisms on a Mobile Botnet over a LTE Network. 11th International Conference on Malicious and Unwanted Software (MALWARE11), Fajardo, Puerto Rico, USA, Pages 1–9, October 2016.

[3] Asem Kitana, Issa Traore, and Isaac Woungang. Towards an Epidemic SMS-based Cellular Botnet. Journal of Internet Services and Information Security (JISIS), Volume 10, Number 4, Pages 38–58, November 2020.

1.5 Thesis Outline

The thesis is organized as follows:

- Chapter 1 presents the motivation and contributions of this thesis.
- Chapter 2 provides some background and related work on the subject topic of this thesis.
- Chapter 3 presents the SMM and AMM mobility models and a study of their impact on the mobile botnet over LTE networks.
- Chapter 4 presents the DBM and SPBM Base Transceiver Station selection mechanisms and a study of their impact on the mobile botnets over LTE networks.
- Chapter 5 presents an epidemic SMS-based cellular botnet and the deployment of various topologies.
- Chapter 6 concludes the thesis and highlights some future work that can be carried further.

Chapter 2

Background and Related Work

In this chapter, we provide background knowledge on the different generations of wireless mobile networks, and present an overview of mobile botnet, its definition, examples, and components. Furthermore, we summarize and discuss related work on mobile botnet.

2.1 Background

2.1.1 Evolution of Wireless Mobile Networks

The development of wireless mobile networks has evolved as a sequence of successive network generations from first to fifth generations. We revisit these different generations in the following subsections.

2.1.1.1 First Generation Networks

The First generation networks (1G), launched in 1979, was analog-based and limited to voice services and capabilities only. Its main characteristics were poor coverage and low sound quality, no roaming support, no compatibility between mobile network operators, limited spectrum efficiency, and calls were not encrypted, so anyone with a radio scanner could drop them. Prominent examples of such systems include the Nordic Mobile Telephone (NMT) system and the Total Access Communications System (TACS) [2] [3]. The

main threats faced by these systems include illegal interception, cloning, and masquerade attacks [4].

2.1.1.2 Second Generation Networks

The Second generation networks (2G), launched in 1991 promised higher capacity and better voice quality than the 1G systems. Representative such systems include the Global System for Mobile Communications (GSM) and the Code Division Multiple Access (CDMA). The main characteristics of 2G are higher data rates for services [5], efficient support of non-real-time packet data traffic, and high level of modulation and coding within the carrier bandwidth [6]. It was also the first time that calls were encrypted and the users could send SMS, pictures, and multimedia messages (MMS) on their phones. The deployment of these systems entail using digital cellular technologies, the Time Division Multiple Access (TDMA) transmission method, and slow frequency hopping for voice communication. The main security threats faced by 2G systems include message spamming for pervasive attacks and injection of false information [4].

2.1.1.3 Third Generation Networks

The Third generation networks (3G), launched in 2001, was a further evolution of GSM systems handled under 3GPP to define the global third generation Universal Mobile Telecommunications System (UMTS), whose main components are the UMTS Terrestrial Radio Access Network (UTRAN) based on Wide-band Code Division Multiple Access (WCDMA) radio technology and the CDMA2000 system, which integrates additional voice and data services to support a variety of broadband data applications such as broadband Internet access and multimedia downloads. Other representative such systems include the High-Speed Downlink Packet Access (HSDPA) system that ensures spectrum efficiency for higher speed data services [7], the High-Speed Uplink Packet Access (HSUPA) system [8] which improves the radio access network for packet connectivity by supporting the IP-based con-

nectivity and software applications. Its main characteristics were that the vendors' network protocols were standardized, making international roaming services become a real possibility for the first time; and the data transfer capabilities were increased (4 times faster than 2G), allowing new services such as video conferencing, video streaming and voice over IP. The main security threats faced by 3G systems include the migration of Internet security vulnerabilities, which were enabled by the IP-based communication [4].

2.1.1.4 Fourth Generation Networks

The Fourth generation networks (4G), launched in 2009, was termed as Long Term Evolution (LTE) Standard. The main characteristics of 4G systems include higher download and upload speeds, improved data rate, fast mobile web access (up to 1 gigabit per second), higher-level data services (such as business applications, audio and video streaming, video messaging, video telephony, and mobile TV), low latency, simple protocol architecture, efficient multicasting and broadcasting services, and compatibility with earlier 3GPP releases [9] [10]. LTE has become the dominant mobile access technology in 2020, and it is estimated to stay the dominant mobile access technology by the end of 2026 as more subscribers migrate to 5G [11]. The main security threats of this technology were the migration of Internet security vulnerabilities observed in 3G systems, but now more exacerbated [4].

2.1.1.5 Fifth Generation Networks

The emergency of the Fifth generation networks (5G) is a result of the current Internet of Things (IoT) networks expansion, coupled with the massive demand on big data systems, which require high data rates and low latency for the mobile data traffic [12]. 5G is expected to provide superior and ubiquitous connectivity, much higher speed and rate, and very low latency. The deployment of 5G networks will facilitate, support, and expand the utilization of a new generation of opulent services and mission-critical applications (such as Augmented Reality (AR), Virtual Reality (VR), industrial robotics and industrial IoT,

and self-driving cars), that were not possible in 4G due to limited bandwidth, latency, and security vulnerabilities [13].

This Thesis focuses on the case where the DDoS attack is launched form multiple machines that are geographically dispersed using mobile botnets. Here, the LTE-based mobile botnets is run by infecting the vulnerable mobile devices in the LTE network, then the infected mobile devices are recruited as bots for launching DDoS attacks to disrupt the availability of multiple components' services inside/outside the considered LTE network.

2.1.2 Mobile Botnet

We are living in an age where mobile devices have become a must and it is not a luxurious gadget. In parallel, a new generation of malware has evolved to strike mobile devices and leverage their popularity to establish mobile botnets.

A mobile botnet is a group of compromised cellular devices that are remotely controlled by a botmaster via a command and control (C&C) channel. The construction of mobile botnets grants attackers the ability to execute multiple malicious actions that allow them to assault the security and privacy of the targeted cellular devices. Examples of such malicious actions are installing new applications, requesting a URL from the mobile device, sending spam, making phone calls, spying on the users, and displaying unwanted messages [14] [15].

A mobile botnet consists of a Botmaster, a C&C server, a C&C channel, and a set of compromised mobile devices (also called bots), as described in the following:

- Botmaster: this is a person or an entity that operates and controls the mobile botnet malicious activities.
- C&C server: this is an online resource that changes or influences the behavior of the bots. It is the way by which a botnet is controlled. In addition, the C&C server hosts the malware components, the bot agents files, and the updates needed for the mobile

botnet operations.

- C&C channel: this represents the interface between the C&C server and the compromised mobile devices, through which the aforementioned entities communicate.

- The compromised mobile device: this is the infected cellular device (also known as bot agent). The main functions of a bot agent are to receive and interpret the commands from the C&C server, and then execute the attacks and send back the data to the C&C server. Examples of mobile botnets are SymbOS.Yxes that targets the Symbian platform [16], Ikee.B that targets the jailbroken iPhones devices [17], GEINIMI that targets the Android platform [18], and ZeuS that targets the Blackberry, Windows, and Symbian mobile platforms [19].

2.1.3 Command and Control Mechanisms

The botmaster in a mobile botnet can control all the compromised mobile devices through the C&C channel. The role of the C&C channel is vital because it represents the interface that allows the botmaster to disseminate the desired commands to the infected machines (bots) and control them. The C&C structure of a mobile botnet could be established based on a centralized or decentralized structure as described in the following.

2.1.3.1 Centralized Structure

Under this structure, all the infected mobile devices of the mobile botnet network are connected to a centralized server, where the malicious commands are issued. This structure offers the botmaster an effective and simple way of communication with the bots. In addition, the centralized C&C channel can be easily managed by the botmaster. In this structure, two types of command dissemination styles prevail: (1) Push style (Real-time control) - where there is always an active connection between the bot agents (i.e. infected mobile devices) and the C&C server. In addition, the bot agents are always in the waiting situa-

tion, watching for commands from the botmaster to be dispatched, such as through Internet Relay Chat (IRC) channels; and (2) Pull style (Non real-time control) - where the bot agent sends a request to the C&C server to get the information and commands; in this case, there is no need to maintain an active connection. Here, periodically, a bot agent can establish a connection to the C&C server and start fetching the new commands like HTTP based C&C. Also, in this approach, the bot agent sends a HTTP request to the C&C web server and receives the commands via a HTTP response.

2.1.3.2 Decentralized Structure

In this structure (also known as Peer-to-Peer (P2P) botnet), there is no central C&C server. Instead, each compromised mobile device in the mobile botnet network plays a dual role, which is that of infected mobile device and C&C server. Therefore, if one of these compromised mobile devices goes down, another agent will be available to take the role of the C&C server. In this kind of structure, a P2P file sharing system is used, which enables a user to download the files using a P2P client from other systems or peers. A file index is used by a P2P client to locate the desired file and peer-to-peer queries for the desired file across the P2P network is operated until the file is found or the query is expired. The discovered file is then downloaded from the closest peers or in segments from multiple peers, depending on the considered P2P protocol. Afterwards, the file segments are reassembled after the download process is fully accomplished by the P2P client.
P2P C&C structures can be categorized into two types based on following mechanisms:

1. C&C mechanism that builds its own P2P network, also known as bot-only P2P botnet.

2. C&C mechanism that uses an existing P2P network, which includes two styles: (a) Parasite style - where all the infected mobile devices are located in the same current P2P network, where bootstrapping (i.e. the process of joining a P2P network) is not

required since all the bots are already part of the network; and (b) Leeching style - where the bots can be any vulnerable mobile device in the cellular network and not just within an existing P2P network. Therefore, some bots that are not part of a P2P network will need to bootstrap to join the P2P network.

In addition to the previously mentioned two C&C mechanisms, also, there is a third mechanism that could be established. This third C&C mechanism is the hybrid C&C structure, which is established by combining both the centralized and decentralized structures.

2.1.4 Mobile Botnet Attacks

Mobile botnets represent a major source of attacks and malicious activities as described in the following.

2.1.4.1 DDoS Attack

DDoS attack is a mechanism that consists of targeting the availability of network services of a victim by sending a huge number of requests from different sources to the victim's network to consumes the victim's resources (i.e. bandwidth, memory, CPU, etc.). This could lead to shutting down the network itself. A DDoS attack represents a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of bogus traffic. This type of attacks is more severe when multiple compromised mobile devices are involved as sources of the attack [20] [21].

2.1.4.2 SMS Phishing Attack

This is also known as Smishing attack (a type of phishing attacks). This category of attacks lies under the umbrella of social engineering attacks. It is defined as a deceptive effort by an attacker to get access to personal information such as user names, passwords, credit cards'

numbers, of victims. Usually, an attacker tries to masquerade as a legitimate party via online communication media using techniques such as email spoofing, instant messaging, and SMS messaging. Typically, the attacker uses cellular phone text messages to deliver the bait, inducing the victim to reveal their personal information. Afterwards, the victim is invited to provide his/her private data [22] [23].

2.1.4.3 Click Fraud Attack

In this type of threats, the attacker creates fake clicks for online advertisements that imitate the valid advertisements style, resulting in some financial compensation to be paid by the advertisers. In transactions involving this type of attacks, a pricing model is usually utilized, which is based on a pay-per-click mechanism, i.e. the revenue for the advertisement platform (such as Facebook or Google) depends on the number of clicks the targeted user has made through the advertisement platform. Unfortunately, several hackers can exploit this model and use botnets to perform fraudulent clicks [24] [25].
This thesis focuses on DDoS and SMS phishing attacks.

2.2 Related Work on Mobile Botnet

While mobile botnet is an emerging field of research, a few proposals have been published in addressing various aspects of this threat. We discuss these proposals in the following.
In [26], Singh et al. have developed a mobile botnet that initiates DoS attack based on bluetooth service and showed that bluetooth can be used as C&C channel by conducting two experiments. The first experiment was based on a large-scale simulation using publicly available bluetooth traces. To emulate the infected mobile devices and the bluetooth functionalities, the Sun Wireless Toolkit was applied to different datasets: the MIT dataset of bluetooth traces of 100 mobile phones and the NUS dataset of bluetooth traces of 12 mobile phones [27]. It was shown that malware in mobile botnet can be propagated over 66% of

the infected nodes within one day. In the second experiment, publicly available traces from the New York City subway system [28] were used to simulate more realistic environments. The outcome of the study indicates that the robustness of the mobile botnet propagation is increased when node popularity is used as key element for designing the C&C channel. In this case, few infected nodes in the mobile botnet can communicate with the botmaster to guarantee the robustness of the mobile botnet. The threat model underlying their proposed mobile botnet involved several assumptions. For instance, it was assumed that defenders have access to malicious binaries of the bots, and limited information were disclosed about the defense mechanisms.

In [29], Zeng et al. studied the malware dissemination in a mobile botnet using SMS service as C&C channel in P2P structure model based on Kademlia and Gia protocols. The proposed scheme involved a mobile botnet architecture made of 200 mobile nodes. In the proposed P2P structure model, a unique key was assigned to each infected mobile node in the botnet, so infected devices can share data based on these unique keys. This model was shown to achieve a successful malware dissemination via a simple SMS word mapping technique. However, a weakness of the proposed model is the fact that the Kademlia protocol implementation requires around 20 SMS messages to achieve an effective and successful propagation, which increases the possibility for detecting the mobile botnet.

In [30], Li et al. proposed a malware propagation scheme that relies on bluetooth service, called Community-based Proximity malware Coping (CPMC). This scheme is based on the concept of community by using social network properties such as contact history and grouping structure, which add levels of permissions to mobile networks. CPMC contains two main types of components. The first one is short-term coping components, which are used to handle and manage the propagation of malware by selecting infected nodes in each community to distribute a malware signature. The second component type is long-term evaluation components, which are used to generate a vulnerability assessment for each individual node based on the observed infection history. In the proposed scheme, the mal-

ware is constructed by simulating nodes' locations based on real traces of bluetooth devices from the MIT Reality Mining dataset, which involves 100 phone devices and the Haggle dataset involving 41 imotes. Also, the malware environment is simulated by using traces from the Florida Atlantic University (FAU) dataset which represents a map of 250 students from four departments at Florida University. The CPMC scheme is neither centralized nor fully-distributed, which gives it an advantage over many of the existing coping schemes of mobile malware. Also the scheme is effective due to the process of implementing a community quarantine method. However, a weakness of the proposed model is using very small number of nodes for designing and testing the effectiveness of the proposed scheme.

In [31], Geng et al. proposed a heterogeneous mobile botnet using SMS service as C&C channel with multi-tree topology. The robustness of the underlying botnet C&C channel is ensured by using a proposed replacement mechanism for failed or recovered bot server node, and by encrypting the critical commands and bots lists in the network. The proposed model, however, remains purely theoretical as no implementation nor experimental validation of the proposed model have been carried out.

In [32], Hua et al. proposed a proof-of-concept for two C&C mobile botnet designs. The first one uses SMS service as C&C channel by implementing a SMS flooding algorithm by using the igraph simulator, and the second design uses bluetooth service as C&C channel by using the NS-2 simulator. The authors used for the SMS-based mobile botnet a uniform random graph topology involving 2000 nodes. It was shown that malware propagation can affect 90% of the nodes in a network in 14 minutes and in this process, each node sends a maximum of 4 messages. In the design of the mobile botnet based on bluetooth, the mobility scenario was implemented by using the Self-similar Least Action Walk (SLAW) scenario. For this model, it was shown that the malware propagation can infect 90% of the nodes in the network within 1 hour even if the infection rate is very low (typically only 20 infected nodes out of the total number of nodes). However, the proposed defense mechanisms does not seem realistic and could potentially be evaded.

In [33], Zhuo et al. studied the impact of mobile botnet propagation by applying a stochastic approach. They found that the average size of the mobile botnet increases quadratically if the coverage range exceeds a threshold. Also, they investigated the risk of initiating a DoS attack based on the proposed mobile botnet, using bluetooth as C&C channel and found that the risk level increases by providing more network bandwidth. The propagation behavior of the proposed mobile botnet was studied by running a simulation, where the UDelModels tool was used to generate realistic human mobility traces. It was demonstrated in the simulation that the propagation mechanism was not efficient due to the fact that the deployment of coverage radius was not sufficiently large. Consequently, this shows that when the coverage radius is not sufficiently large, there is an exponential decay in the mobile botnet size which means that the malware could infect only a limited number of nodes.

In [34], Traynor et al. studied the impact of designing a mobile botnet that launches a DoS attack against the core of a GSM (Global System for Mobile Communications) cellular network services by targeting the Home Location Register (HLR). Using the Telecom One (TM1) tool, the Maximum Qualified Throughput (MQTh) of traffic between different mobile devices in the GSM cellular network was measured by simulating GSM MAP (Mobile Application Part) operations. These operations contain two parts. The first part is READ operations where phone calls are made and text messages are sent, and the second part is WRITE operations where the users are authenticated in the network. The results of the study showed that the process of compromising WRITE commands consume more bandwidth compared to the process of compromising READ commands, and therefore the WRITE commands have a higher severity impact than the READ commands in a GSM cellular network.

In [35], Karim et al. conducted a comprehensive review on mobile botnet attacks by studying the attack vectors of mobile botnet in a thematic taxonomy. Although the survey doesn't introduce any new results, it gives insight into the different categories of mobile botnets.

In [36], Khosroshahy et al. studied the impact of a mobile botnet that launches a DDoS attack against the air interface of 4G core network. In their experiment, the DDoS attack mechanism is activated by enforcing the infected mobile devices in the cellular network to dispatch multiple requests through the Uplink and Downlink channels of the air interface of the 4G core network. As a result, a congestion is established on the air interface, which leads to overwhelming the 4G network resources and services. Simulations conducted by using the LTESim framework simulator show that a mobile botnet that can infect only 6% of 4G network subscribers can effectively cause an outage in the cellular network services. However, the obtained simulation results are valid and applicable when the mobile botnet initiates the DDoS attack in peak hours and emergency situations only.

In [37], Szongott et al. investigated some features of new smartphones that allow the propagation of mobile malware in Wi-Fi network environments, by proposing a mobile malware prototype that leverages two features of mobile phones, namely, automatic reconnection for known Wi-Fi access points and captive portals. Through simulation, it was shown that the proposed mobile malware is capable of infecting other devices in the Wi-Fi network by deploying bogus Wi-Fi access points that don't require any authentication mechanism (e.g. user name and password). If a mobile device tries to access the Internet by connecting to the bogus Wi-Fi access point in the network, then the mobile device will be infected. However, the simulation was conducted by using the mobile security and privacy toolkit simulator, which is built and designed by the authors rather using one of the existing benchmark simulators.

In [38], Gorbil et al. investigated the severity levels of mobile botnets that initiate Dedicated Channel (DCH) attack and Forward Access Channel (FACH) attack against the radio resource control (RRC) layer of the UMTS cellular network. In the DCH attack, the botmaster aims to overload the control plane of the UMTS network air interface by sending fake signalling messages that generate redundant requests to the CELL_DCH state of RRC, which consumes the bandwidth of the Uplink and Downlink channels of the air interface.

While in the FACH attack, the botmaster floods the air interface with bogus signalling messages that generate redundant requests to the CELL_FACH state of the RRC, which also consumes the bandwidth of the Uplink and Downlink channels of the air interface. Triggering the DCH and FACH attacks against the air interface of the UMTS networks leads to reducing the quality of services, and furthermore stopping network services. The simulation was conducting by using the OMNeT++ simulation framework.

In [39], Merlo et al. proposed a mobile botnet model that can initiate a DoS attack against the UMTS core network by recruiting SIM-less mobile devices, which are mobile devices that don't employ Subscriber Identity Module (SIM) cards. In their experiment, the mechanism of deploying the DoS attack is based on creating a database of multiple valid and unique International Mobile Subscriber Identity(IMSI) identifiers by the attacker, then flooding the UMTS network with multiple attachment requests to the HLR (Home Location Register) database, where each request requires a valid and unique IMSI identifier, which eventually leads to consume the HLR resources and degrade the quality of UMTS network services. However, the experiment was conducted by using an envisioned attacking mobile device, equipped with multiple UMTS radio interfaces and has no SIM modules, which doesn't represent the reality of mobile devices architecture.

A state-of-the-art comparison between different authors for the mobile botnet construction is conducted in Table 2.1.

A notable point should be highlighted in Table 2.1, that the LTE network is deployed as C&C mechanism in our proposed mobile botnet and also in the proposed mobile botnet of Khosroshahy et al. study in [36]. The main difference between the two models is that in our approach we are using the LTE network as C&C mechanism to attack a victim server outside the LTE network architecture (i.e. targeting the web server in the Internet). While in [36], the LTE network is used as C&C mechanism to attack the internal components of the LTE network architecture (i.e. targeting the air interface of LTE core network).

Table 2.1: Comparison of different mobile botnet designs.

Author	**C&C Mechanism**	**Attack Model**	**Simulation Tool**
Singh et al. [26]	Bluetooth	DoS attack	Sun Wireless Toolkit
Gorbil et al. [38]	UMTS	DCH/FACH attacks	OMNeT++
Zeng et al. [29]	SMS messages	Flooding attack	OverSim
Khosroshahy et al. [36]	LTE	DDoS attack	LTESim Framework
Hua et al. [32]	Bluetooth and SMS messages	SMS phishing	NS-2 and igraph
Li et al. [30]	Bluetooth	Flooding attack	Trace-driven
Zhuo et al. [33]	Bluetooth	DoS attack	UDelModels
Traynor et al. [34]	GSM	DoS attack	Telecom One (TM1)
Merlo et al. [39]	UMTS	DoS attack	SIM-less device
Geng et al. [31]	SMS messages	Flooding attack	Math analysis
Szongott et al. [37]	WiFi	Evil Twin attack	Mobile Security and Privacy Toolkit
Kitana et al. [40]	LTE	DDoS attack	Riverbed
Kitana et al. [41]	LTE	DDoS attack	Riverbed
Kitana et al. [42]	SMS messages	SMS phishing	igraph

Chapter 3

Impact of Mobility Models on Mobile Botnet

In the recent years, mobile telecommunication networks and systems have witnessed a rapid evolution in terms of development, deployment and application services. The explosion of the number of mobile cellular users, coupled with the need for higher data rates, lower transmission latency, increased signal range, and higher efficiency, have motivated the advent of the Long Term Evolution (LTE) technology for 4G telecommunication systems. With this advantage also comes some security concerns with regard to a variety of attacks that can be launched on these systems. For instance, attackers can establish a mobile botnet to conduct several types of cyber attacks on LTE-based networks. This Chapter studies the impact of a mobile botnet on a LTE network by implementing a mobile botnet architecture that initiates a DDoS attack.

3.1 Considered Approach

In order to understand the behavior of the mobile botnet and the factors that affect its operations and propagation, we have studied the impact of cellular devices' mobility dynamics on the mobile botnet operations over a LTE (4G) cellular network. Specifically, we have studied the performance of a mobile botnet by deploying two different mobility models to

simulate the movements of cellular devices in the mobile botnet. The first model is based on the Random WayPoint (RWP) model which we refer to as Symmetric Mobility Model (SMM). This model represents the uniform movement patterns of cellular devices in a mobile botnet. The second model is a mobility model based on real trajectory traces of taxi cabs from the Shanghai Dataset [43] which we refer to as Asymmetric Mobility Model (AMM). This model represents the random movement patterns of cellular devices in a mobile botnet.

3.2 LTE Network Architecture

The 3GPP Telecommunication Standards Group [44] in its release 8 has introduced the concept of the Evolved Packet System (EPS), a high-level architecture of the LTE technology. This architecture is composed of three key components, namely, the evolved UMTS terrestrial radio access network (E-UTRAN), the user equipment (UE), and the evolved packet core (EPC), which are interconnected to each other through different interfaces (so-called air interface (Uu), S1 interface, and SGi interface) as shown in Fig. 3.1. It also enables the interconnection of the LTE network with other 3GPP and non-3GPP systems.

The LTE architecture contains only the Packet Switched (PS) domain, where each stack of the E-UTRAN and EPC has an IP address, enabling the LTE network components and the stacks to communicate with each other over the underlying IP transport network. As shown in Fig. 3.1, each component of EPS has its own internal architecture and the E-UTRAN component has only one stack (so-called eNodeB (eNB) station) that controls the radio communications between the user equipment (UE) (such as mobile devices) and the EPC component. A UE can be connected to one eNodeB and one cell at a time and the eNodeB station that serves a UE is referred to as serving eNodeB.

Typically, the eNB sends the user data and low-level signaling commands (also called han-

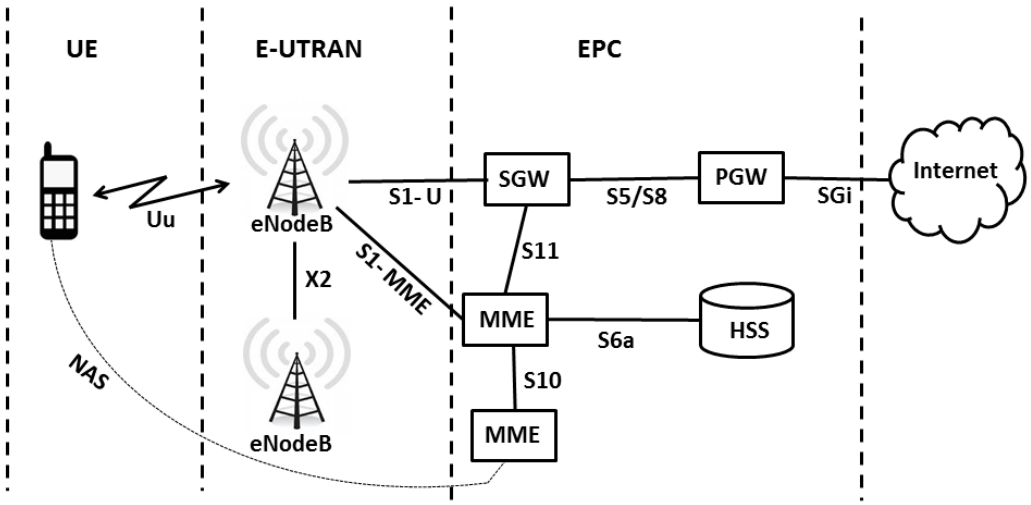


Figure 3.1: EPS architecture of the LTE network [2].

dover commands) to its mobile devices on the downlink channel and receives the data from mobile devices on the uplink channel using the air interface (Uu). Each eNB station is connected to the EPC through the S1 interface by using the S1-U and S1-MME. It can also be connected to other eNB stations through the so-called X2 interface.

On the other hand, the EPC component is made of four stacks, namely the Home Subscriber Server (HSS), the Mobility Management Entity (MME), the Packet Data Network Gateway (PGW), and the Serving Gateway (SGW). The MME is meant to control the high-level operations of mobile devices in the LTE network by sending some signaling messages related to security control, tracking area management, mobility between the different 3GPP access networks, and EPS bearer management. The SGW controls the process of data packets forwarding and routing between eNB and PGW stacks, where the PGW acts as a contact point linking the EPC and the external packet data networks (so-called PDNs) through the so-called SGi interface. Each PDN has a unique identifier called Access Point Name (APN) which allows the connection between the mobile devices and different PDNs. The last stack of the EPC component is the HSS, a database server that contains the information related to LTE network subscribers.

In the EPS architecture (Fig. 3.1), the air interface is composed of two levels: the non-

Access Stratum (NAS) level and the Access Stratum (AS) level, which are meant to facilitate the exchange of signaling messages between the MME stack and the UE stack using the EPS session management (ESM) and the so-called EPS mobility management (EMM) protocols. The NAS level hosts the high-level signaling messages, which are then transported via the AS protocols of the Uu and S1 interfaces as shown in Fig. 3.2.

The 3GPP standard for the radio access of LTE system is designed to operate in two phys-

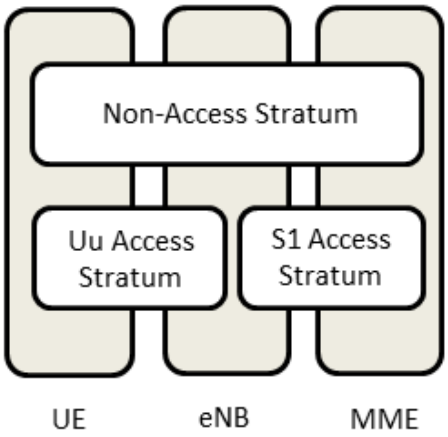


Figure 3.2: AS and NAS on the air interface of LTE

ical layer duplex schemes: the Time Division Duplex (TDD) and the Frequency Division Duplex (FDD) [45]. In the FDD scheme, a UE transmits the data (uplink) and receives it (downlink) by using two different channels, one for the uplink traffic and the other for the downlink traffic. On the other hand, in the TDD scheme, both the uplink and downlink traffic share the same channel using different time slots. The LTE system can support up to six channel bandwidths, namely channels with 1.4, 3, 5, 10, 15, and 20 MHz [46]. In addition, the establishment of connections between the UE and EPC is achieved by means of the so-called EPS bearer [47] as shown in Fig. 3.3, which are activated by means of the GPRS Tunnelling Protocol (GTP).

In this thesis, the LTE network acts as an infrastructure network for running the operations of the mobile botnet architecture. The standard LTE module available in the Riverbed Modeller [48] is used to build a LTE network, whose components and parameters are described

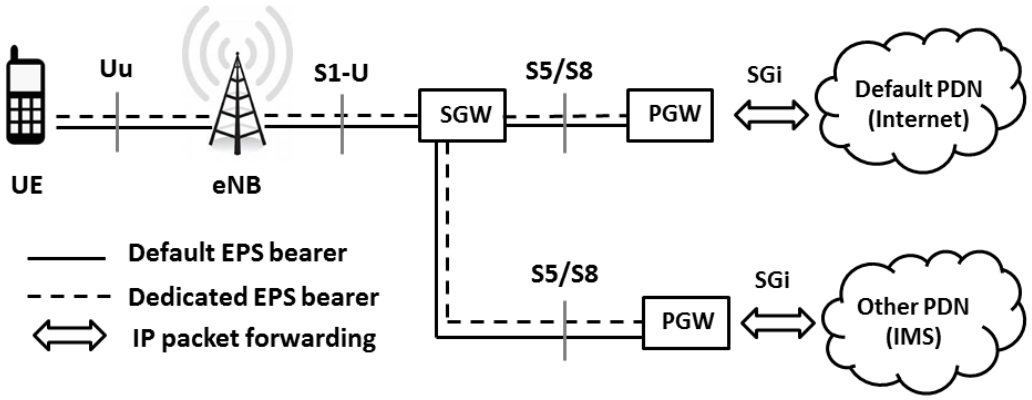


Figure 3.3: The default and dedicated EPS bearers using an S5/S8 interface based on GTP

as follows.

3.2.1 EPS Bearer Activation

Two EPS bearers are configured and implemented in each mobile device, namely: (1) a non-GBR default bearer - which is used to transfer the web application services (here HTTP traffic) to an E-commerce server deployed in the mobile botnet architecture, and (2) a GBR-based bearer - which is meant to serve for video service traffic that is present at the e-commerce web site. As per the standardized QoS Class Identifier (QCI) characteristics table of 3GPP TS 23.203 [44], we have considered QCI8 and QCI2 for the default and dedicated bearers, respectively, and their values are shown in Table 3.1. In Table 3.1, the QCI parameter defines four metrics for classifying the QoS for EPS bearers, namely, resource type, QCI priority, packet delay budget, and packet error (or loss rate). This parameter is set through the LTE configuration manager submodule of the LTE module. In doing so, the GBR-based bearer has a guaranteed minimum rate and is required to be checked by the admission control process when its radio bearers are created. On the other hand, the non-GBR bearer is considered as the best effort bearer with no resource guarantee.

The QCI priority is meant to determine the order in which the data packets should be transmitted. The packet delay is considered as the maximum time that a packet is used when transiting via the MAC and radio link control layers in the network. This can be interpreted

Table 3.1: 3GPP TS 23.203 Standardized QCI characteristics [2].

QCI	**Resource type**	**QCI priority**	**Packet delay**	**Packet error loss rate**	**Services**
1	GBR	2	100 ms	10^{-2}	Conversational voice
2	GBR	4	150 ms	10^{-3}	Real-time video
3	GBR	3	50 ms	10^{-3}	Real-time games
4	GBR	5	300 ms	10^{-6}	Buffered video
5	Non-GBR	1	100 ms	10^{-6}	IMS signaling
6	Non-GBR	6	300 ms	10^{-6}	Web, email, FTP (high priority users)
7	Non-GBR	7	100 ms	10^{-3}	Voice, real-time video and games
8	Non-GBR	8	300 ms	10^{-6}	Web, email, FTP (mid priority users)
9	Non-GBR	9	300 ms	10^{-6}	Web, email, FTP (low priority users)

as a maximum delay with a confidence level of 98%. The packet error loss rate represents the maximum ratio of Layer-2 packets that have not been successfully delivered. The activation/deactivation of an EPS bearer is made according to the specifications provided in [49]. Typically, a UE triggers the creation or activation of a bearer by establishing a communication with the Evolved Packet Core (EPC) node using an EPS session management (ESM) bearer resource modification request message [49], and an eNodeB is used to deactivate the bearer and free up its radio resources when needed.

3.2.2 GPRS Tunneling Protocol

In the proposed LTE network, the EPS bearers are managed by means of the GPRS Tunnelling Protocol (GTP) tunnels as shown in Fig. 3.4. Basically, a GTP tunnel is dynamically established for each EPS bearer in the S1 and S5/S8 interfaces of the LTE network User part (GTP-U) layer of the protocol stack operating in the PDN Gateway, eNodeB (eNB), and Serving Gateway (i.e. SGW) nodes. For data to be sent by the UE to the Web server, the IP datagrams (which also contain the IP address of the mobile device) are sent through the corresponding GTP tunnels, along with their layered encapsulation headers (as shown in Fig. 3.5) until they reach the Web server. While in transit, the PGW interface is used to confirm the correctness of these IP addresses, and the SGW interface is used to perform their routing to the Web server. A similar process is used to send the data packets from the Web server to the eNB.

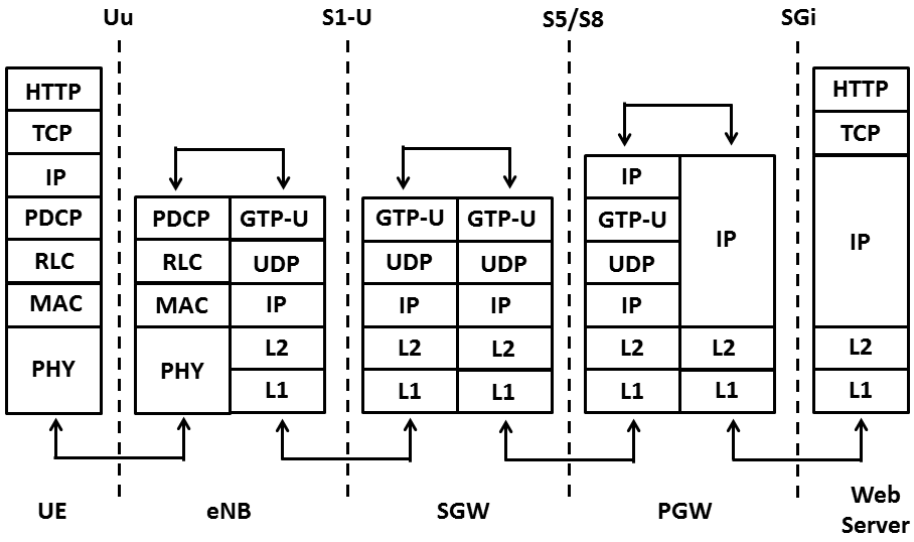


Figure 3.4: Protocol used for data exchange between mobile devices and Web server [2].

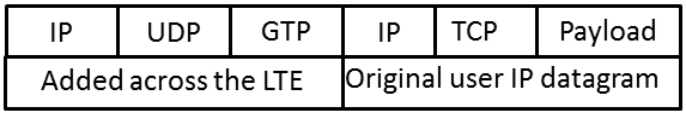


Figure 3.5: IP datagram encapsulation.

3.2.3 User Equipment Architecture

In our proposed LTE network, each node (i.e. mobile device) is enabled to run the following four EMM states as illustrated in Fig. 3.6, which are implemented according to the specification provided in [49]:

1. *Off State*: A UE is in this state when it is switched off, therefore it is not connected to a LTE network.

2. *EMM_Deregistered State*: A UE is in this state when it is initiating the EMM Attach procedure with the EPC [44] or is waiting to finish it.

3. *EMM_Connected State*: A UE enters this state when the registration and attachment procedures [49] are completed.

4. *EMM_Idle State*: A UE enters this state when it is inactive and cannot achieve a significant power saving.

In the Idle state, a mobile device is enforced to move to the Deregistered state and initiate an EMM Attach procedure in one of the following three cases: (i) there is uplink traffic to be sent to the core network; (ii) there is downlink traffic to be received from the core network; and (iii) a UE has initiated a tracking area update procedure [44]. It should be noted that the core network can identify the location of a UE when operating only in two states, i.e. connected and idle states.

3.2.4 Cell Search and Selection

In the proposed LTE network, an EPC component can serve multiple eNB stations, each of which can serve multiple mobile devices. The cell search and selection process is performed during the EMM Attach procedure [49], providing that a mobile device selects a home public land mobile network (HPLMN) to register with. The cell search process is

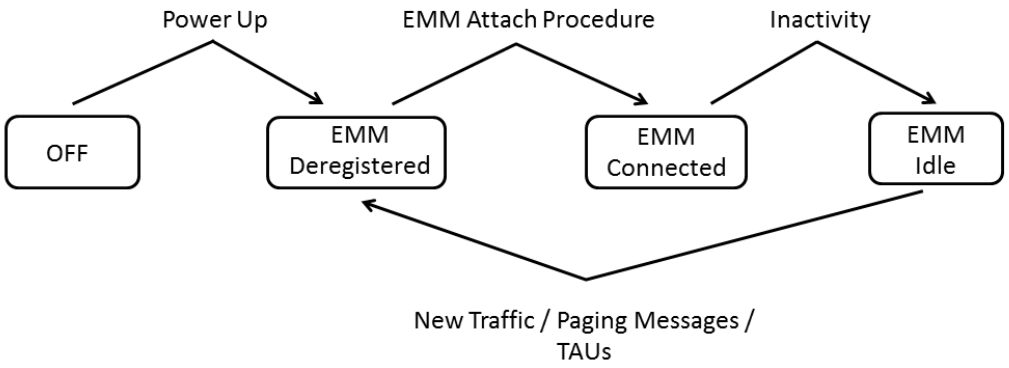


Figure 3.6: EMM UE states.

only performed for that configured HPLMN (i.e. serving EPC). Once the EPC has been selected, the mobile device selects a suitable cell by scanning all the downlink frequencies of all the eNodeB stations that serve this EPC, according to the following criterion $Q_{rxlevmeasured} > Q_{rxlevmin}$, where $Q_{rxlevmeasured}$ denotes the reference signal received power (RSRP) of the cell, i.e. the average total received power, and $Q_{rxlevmin}$ is the minimum value of RSRP that is advertised by an eNodeB station. In our simulations, we have considered $Q_{rxlevmin} = -128$ dBm as suggested in [50]. The RSRP is supported for each eNodeB in the LTE network, where the physical layer updates the RSRP value every 5 ms. The received power RP is obtained as

$$RP = P_{tx} \times G_{tx} \times \left(\frac{\lambda^2}{16\Pi^2 r^2}\right) \times G_{rx} \tag{3.1}$$

where P is the transmit power, G is the directional antenna gain, λ is the wavelength of the signal, r is the distance between nodes, and the subscript tx indicates the transmitter, and rx indicates the receiver. It should be noted that the reference signals are not transmitted nor received, therefore, the RSRP measurement is performed based solely on the primary and secondary synchronization signals.

3.2.5 Handover Mechanism

In the proposed LTE network, the handover process is initiated and controlled by the eNodeB with the assistance of the mobile devices. Also, the handover between the cells using the S1 and X2 interfaces are supported, as well as the Layer-3 RSRP measurement. In our simulations, the mobile device obtains the latest RSRP measurement every 200 ms from the physical layer and updates its Layer-3 measurement module according to the specifications provided in [51]. Also, periodic reports are sent by mobile devices to their serving eNodeB nodes every 240 ms. When the reported measurement by a mobile device violates the handover, another serving eNodeB is appropriately selected, then the original serving eNodeB initiates a X2-handover procedure with the newly selected eNodeB if a X2 interface is available; otherwise, a S1-handover procedure is initiated. Then the selected eNodeB accepts the mobile device if at least one non-GBR bearer is accepted (this is referred to as *the preparation phase*). Assuming that this has happened, the serving eNodeB will send a handover command message to the mobile device to transfer the data packets to it (this is referred to as *the execution phase*). These preparation and execution phases of the handover procedure are deployed based on the 3GPP standard procedure described in [49].

3.2.6 Physical Layer Configuration

In the proposed LTE network, the orthogonal frequency division multiplexing (OFDM) scheme is supported, where each resource block (RB) consists of 12 sub-carriers of 15 KHz, with a length of one slot. Each slot has a time of 0.5 ms and contains 7 OFDM symbols, so one RB has 84 resource elements as shown in Fig. 3.7.

The allocation unit of one subframe is 1 ms in length, which is the minimum allocation unit used by the scheduler to determine the allocations on a frame as per the 3GPP standard [44]. In the air interface of the LTE network, we have considered the LTE-FDD based frame structure type [44], by deploying a FDD profile as a duplexing scheme with a frame

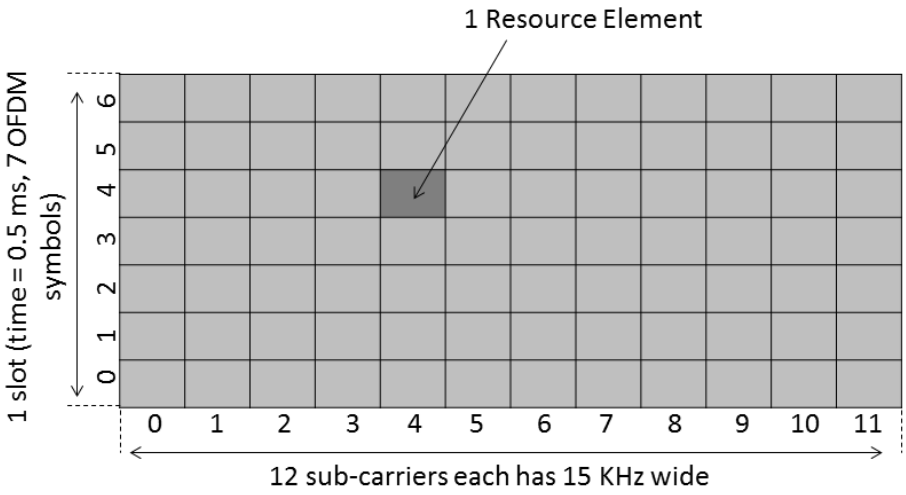


Figure 3.7: A resource block of the proposed LTE network.

length of 10 ms, a slot length of 0.5 ms, and a subframe length of 1 ms. In LTE-FDD based schemes, different channel bandwidths can be supported, namely, 1.4, 3.0, 5.0, 10.0, 15.0, and 20.0 MHz. Their respective numbers of resource blocks (NRB) [44] are shown in Table 3.2. For our simulations, we have considered the channel bandwidth of 20 MHz with $NRB = 100$. The base frequency of the uplink channel (resp. downlink channel) is set to 1920 MHz (resp. 2110 MHz). In addition, in the proposed LTE network, the following physical channels are configured:

- Primary broadcast channel: this is meant to send the primary synchronization signal, secondary synchronization signal, and master information block messages. For these messages, it is ensured that the packet reception is always successful.

- Physical random access channel: this is meant to carry the random access preambles needed for initializing the random access procedure. A contention-based random access mechanism is implemented in our LTE network to prevent the collision between preambles from different mobile devices.

- Physical downlink shared channel: this is meant to transfer the downlink data messages and system information block messages.

- Physical downlink control channel: this is meant to forward the downlink control information messages.
- Physical uplink control channel: this is meant to transfer the uplink control channel messages.
- Physical uplink shared channel: this is meant to transfer the uplink data messages.

Table 3.2: Channel bandwidth parameters.

Channel bandwidth (MHz)	**Number of Resource Blocks (NRB)**
1.4	6
3.0	15
5.0	25
10.0	50
15.0	75
20.0	100

3.3 Considered Mobility Models

To understand the behavior of the proposed mobile botnet and factors that can affect its operations and propagation, we have studied the impact of cellular devices' mobility dynamics on the mobile botnet operations on the proposed LTE network. Two different mobility models are used to simulate the movements of mobile devices in the mobile botnet, namely a symmetric mobility model (SMM) - which represents the uniform movement patterns of mobile devices in the mobile botnet, and an asymmetric mobility model (AMM), which represents the random movement patterns of cellular devices in a mobile botnet. The AMM model is based on real datasets from taxicab deployments in Shanghai [52] whereas, for

the SMM model, a trajectory file generated by the Random WayPoint (RWP) model [48] is used as a movement trajectory file for all cellular devices.

3.3.1 SMM Model

The SMM model is derived from the RWP model. In this model, each mobile device chooses at random a waypoint w in the LTE network deployment region G and moves to its waypoint with a velocity v chosen randomly in the interval $[v_{min}, v_{max}]$, where $v_{min} > 0$ and $v_{max} < \infty$. When a mobile device reaches its waypoint, it remains static for a pre-defined pause time t_p, then starts to move again according to the same process. In doing so, the movement period of a mobile device is indexed by a discrete-time parameter i and a continuous time t. Therefore, the RWP model is represented by a stochastic process $\{(W_1, T_{p1}, V_1), \ldots, (W_i, T_{pi}, V_k), \ldots\}$, where W_i represents a waypoint in G, T_{pi} is the pause time in the waypoint W_i, which is set to 100 seconds, V_i is the velocity of the mobile device during the movement period i where $i \in \mathbb{N}$. All waypoints W_i are distributed randomly using a uniform distribution over the deployment region G, except for W_0, which is generated by using an initial spatial node distribution $f_{ini}(x)$ to randomly place the mobile devices in the LTE network deployment region G at the start of the simulation. The movement vector from w_{i-1} to w_i is defined as a segment (S_i); therefore, the complete movement trace of a mobile device (i.e. its trajectory) is defined as the sequence of these segments, i.e. $\{S_1, \ldots, S_i, \ldots\} = \{w_1 - w_0, \ldots, w_i - w_{i-1}, \ldots\}$.

In our simulations, the RWP movement model is activated by defining G as a rectangular region and by specifying the x-y coordinates, according to the following parameters:

- G_{XMin}: this is used to specify the left (west) border of the movement area on the x-axis of G.
- G_{XMax}: this is used to specify the right (east) border of the movement area on the x-axis of G.

- G_{YMin}: this is used to specify the lower (south) border of the movement area on the y-axis of G.
- G_{YMax}: this is used to specify the upper (north) border of the movement area on the y-axis of G.

Table 4.6 shows the configuration of these parameters. To ensure that all mobile devices

Table 3.3: Parameters of the RWP model.

Parameter	**Value**
G_{XMin}	-2,500 meter
G_{XMax}	4,000 meter
G_{YMin}	-2,598.076 meter
G_{YMax}	2,598.076 meter
Speed	5 meters/second
Pause Time	100 seconds
Starting Time	Time that the simulation starts
Stopping Time	Time that the simulation ends

in the LTE network follow the same movement during simulation, the following steps are taken:

- Before creating the RWP profile, the record trajectory attribute is enabled, which is a feature that allows the trajectory movement of all or specific mobile devices in the deployment region G to be recorded.
- After the RWP profile deployment, the record trajectory attribute value in one of the mobile devices is enabled, so that its trajectory movement can be recorded and saved.
- Next, the assigned RWP profile is deleted from all the mobile devices and the recorded trajectory file to all mobile devices is re-assigned.

An example of a RWP trajectory file (so-called segment-based trajectory) is shown in Fig. 3.8. It consists of 8 segments $\{S_1, \ldots, S_8\}$, where the segment length (l_i) is expressed as

$l_i = \|S_i\| = \|w_i - w_{i-1}\|$. Each segment has a destination waypoint w and an associated starting waypoint r.

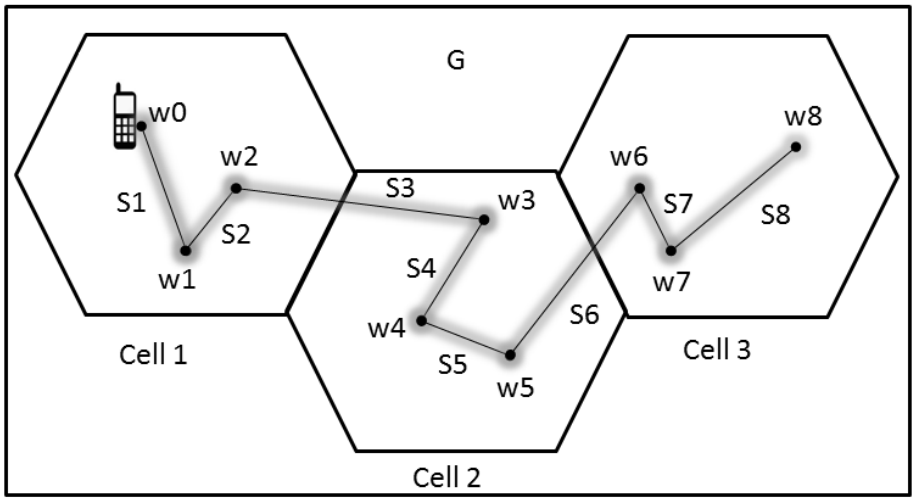
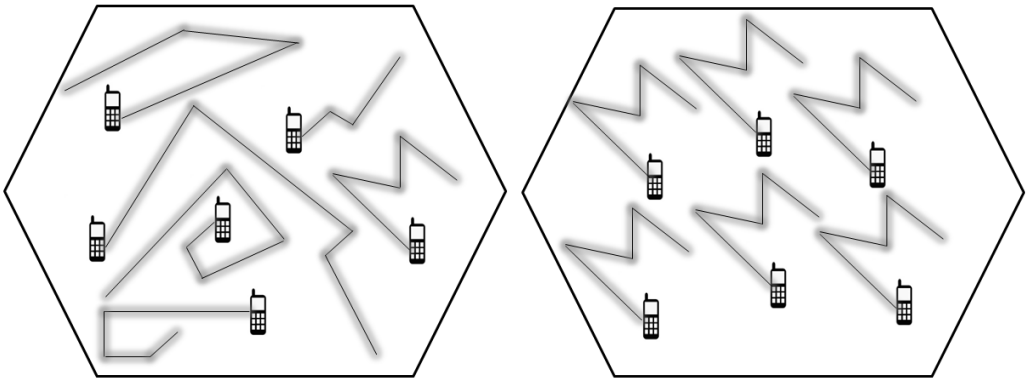


Figure 3.8: Example of a RWP segment-based trajectory.

3.3.2 AMM Model

Unlike the SMM model which assigns the same RWP trajectory file to all the mobile devices in the LTE network, the AMM model is deployed by assigning a different trajectory file to each mobile device. This model represents different random mobility patterns of mobile devices. An example showing the difference between AMM and SMM models using six mobile devices in a LTE cell is shown in Fig. 3.9. For this example, the trajectory paths in an AMM cell are illustrated in Fig. 3.9a and similar trajectory paths in a SMM cell are depicted in Fig. 3.9b. The mechanism for deriving the trajectory files in the AMM model and assigning each mobile device a unique trajectory path is conducted by using the Shanghai dataset [52], which simulates the reality of the mobility movements of all mobile devices in the proposed LTE network. This dataset was collected in Shanghai, China, and involved 5631 taxi cabs. A GPRS-based GPS device in each taxi cab was used to collect and send the location information (i.e. longitude and latitude) to a central server every 5 seconds. The dataset contains 5631 GPS trajectory files as text files (.txt), each containing



(a) AMM model. (b) SMM model

Figure 3.9: AMM vs. SMM models.

hundreds of location instances of a taxi, each of which consists of 7 entries as shown in Table 3.4. The taxi trajectory files are implemented as segment-based trajectory files, in

Table 3.4: Taxi Cab location information from the Shanghai dataset.

Field	**Description**
Taxi ID	Integer identifying the taxi cab
Timestamp	includes date and time as YYYY-MM-DD HH:MM:SS
Longitude	longitude position degree of the taxi cab.
Latitude	latitude position degree of the taxi cab.
Speed	instantaneous speed of the taxi at the moment of taking the GPS coordinate position.
Angle	the angle from the north in the clockwise direction with a unit of 2 degrees.
Status	shows if a taxi cab has a passenger or not (1 = occupied, 0 = free).

which the movement is determined using a series of predefined points defining the mobile device site's movement and orientation along a three-dimensional path (i.e. longitude, latitude, and altitude). In this setting, the altitude field is set to zero to mean that it is inactive in our simulations.

To make use of the segment-based trajectory functionality, the trajectory file should be identified in the ASCII format with a (.trj) suffix. Therefore, each text file (.txt) of the taxi

dataset is converted into a (.trj) file, then each trj file is assigned to a mobile device site's trajectory attribute. During the simulation, a mobile device site follows its trajectory path by moving from one defined point to the next. At any given time, the mobile device position is determined by interpolating between the segment points before and after that time. A segment-based trajectory specifies a mobile device's site location for a finite time duration; if the simulation continues beyond the last specified time in the trajectory, the mobile device remains at the trajectory's endpoint. Each point of a segment-based trajectory has a specified x-y position, altitude, wait time, segment traversal time, and orientation points (i.e. pitch, roll, and yaw). All these values specify the mobile device site's movement in the segment that ends at that point. For instance, the wait time causes a mobile device site to pause at that point before it begins traversing the next segment.

3.4 Mobile Botnet Architecture

To study the behavior of the proposed mobile botnet, we have designed a mobile botnet architecture that initiates in the attack phase a DDoS attack against a HTTP server (web server) considered as the victim server in our scenario. This server can host various sites; for instance, an e-commerce site in our case. As an overlay network, the proposed mobile botnet is composed of four main building blocks, namely, Botmaster, C&C server, LTE infrastructure network, and mobile devices, as shown in Fig. 3.10.

In Fig. 3.10, the Botmaster is the attacker that controls all the infected mobile devices (or bots) through the C&C server. The C&C server acts as an interface that the Botmaster uses to send some commands to the infected mobile devices and control them. The C&C server uses the push mode as a command dissemination mechanism. For simulation purpose, the proposed mobile botnet architecture is composed of 10 hexagon LTE cells, each of which contains one eNodeB station and 50 mobile devices as shown in Fig. 3.12. The eNodeB stations are connected to one EPC station, each of which is configured to represent

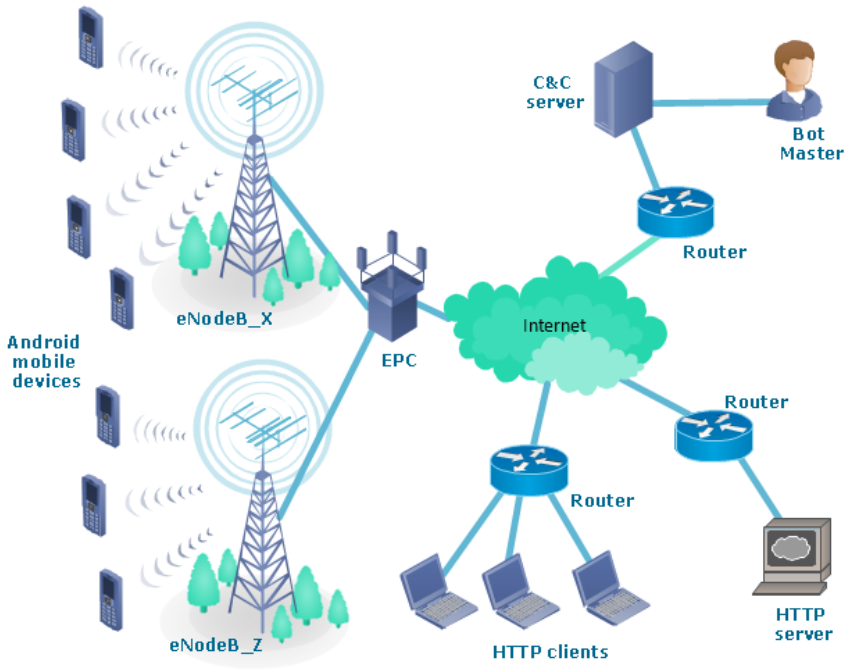


Figure 3.10: Proposed mobile botnet architecture.

the IP-based network of the LTE architecture, itself acting as a gateway to the external PDN (in our case, the Internet). This PDN contains the Botmaster node, the C&C server station, the victim Web server, and routers that interconnect these nodes together with the LTE network as shown in Fig. 3.11. Each LTE cell is configured with a 20 MHz FDD profile and a radius of 1 km. The other simulated parameters of the LTE network are defined based on the aforementioned LTE configuration.

To study the impact of the mobility dynamics on the mobile botnet's behavior, two similar copies of the same mobile botnet topology (Fig. 3.11) are created. In the first copy, the mobility model parameters of the 500 mobile devices are determined based on the SMM model whereas, in the second copy, these parameters are determined based on the AMM model. An additional factor called ratio of infection $RI = NI/Tot$, where NI is the number of mobile devices that are infected and Tot is the total number of mobile devices in the LTE network. To study the impact of this factor on the mobile botnet's behavior, all mobile devices are configured using three different RI values as shown in Table 3.5.

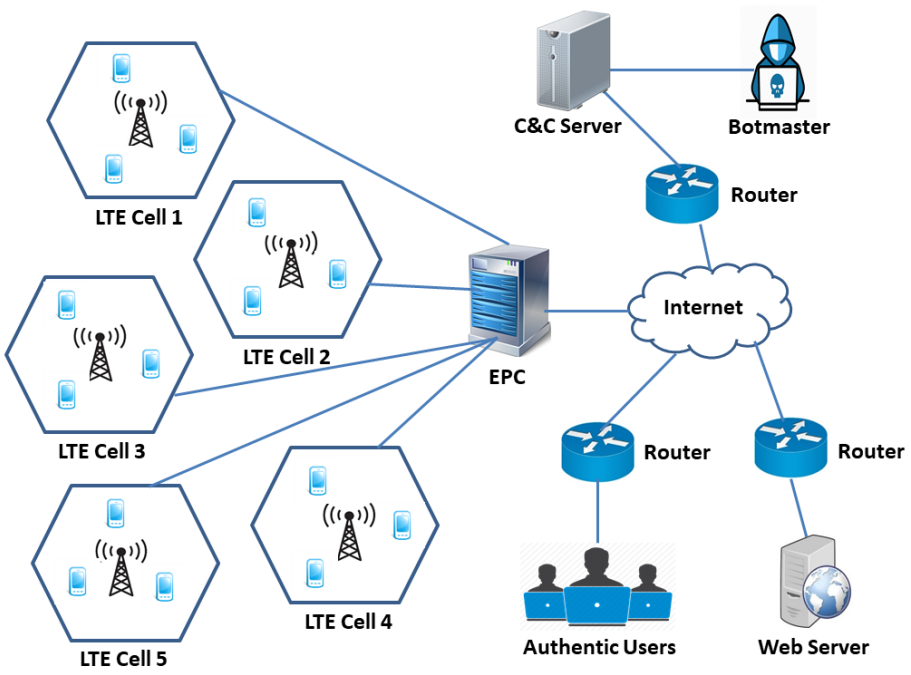


Figure 3.11: Mobile botnet topology.

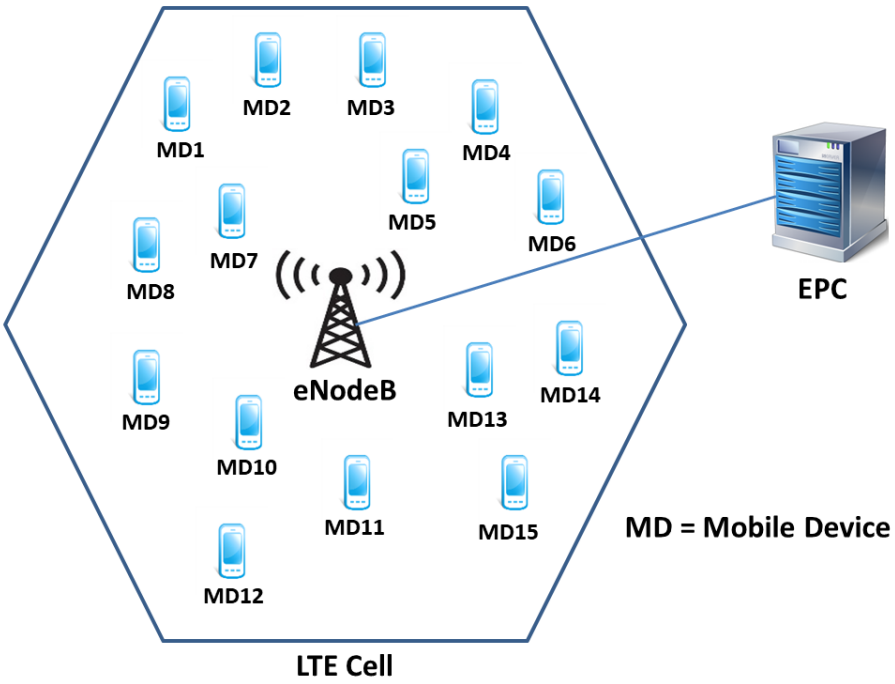


Figure 3.12: Example of a LTE cell.

The C&C server plays its role in the mobile botnet by sending two commands

Table 3.5: Number of infected mobile devices

$NIRI$	0.8	0.5	0.2
AMM-NI	380	277	176
SMM-NI	300	197	96

to all mobile devices in the LTE network, the mechanism of the C&C server in the mobile botnet relies on the following main processes:

- Scanning process: scans all the mobile devices in the LTE network to identify the vulnerable ones.
- Infection process: Identifies all the successfully infected mobile devices.
- Reporting process: Sends the data concerning all infected devices back to the Botmaster.
- Execution process: Executes the DDoS attack against the victim's web server.

It is assumed that all mobile devices in the mobile botnet architecture are Android based, and can be vulnerable to malware attacks such as a Trojan horse, which can be used by the Botmaster to control them. The installation of the malware script on the Android mobile devices is done by repackaging, update attack, or drive-by download [53]. In addition, five HTTP clients are deployed in the botnet architecture, which represent legitimate customers sending genuine HTTP requests to the victim Web server. The process used for differentiating between genuine and attack traffics is described in the sequel.

A DDoS attack is simulated in the attack phase of the mobile botnet over the LTE network as shown in Fig. 3.13. In this attack model, the C&C server (controlled by the Botmaster) starts the attack by scanning all the 500 mobile devices of the LTE network in order to identify the ones that are vulnerable. Upon completion of the scanning process, the C&C server sends a command to infect the maximum possible number of vulnerable

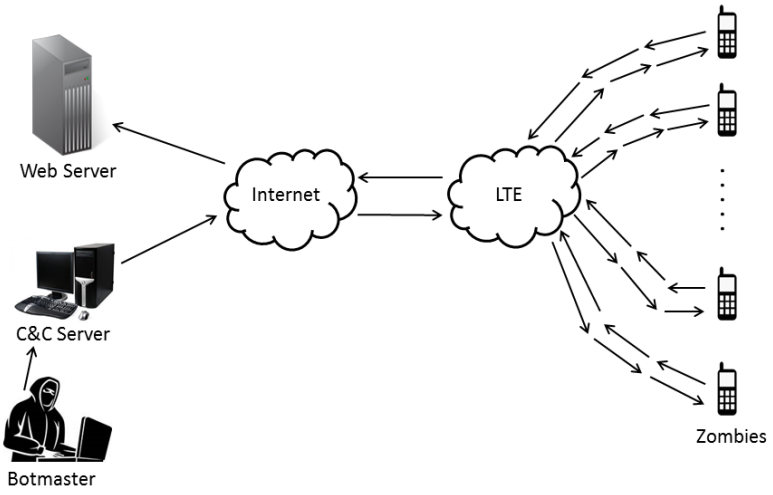


Figure 3.13: Mobile botnet DDoS attack model.

devices using malware already installed on the mobile devices through repackaging, update attack, or drive-by download [53] as per the following steps:

- All mobile devices are configured using three different RI values as shown in Table 3.5.
- Based on the activated RI parameter, the Botmaster receives a report message indicating the value of NI.

Each mobile device infected successfully sends back a notification message to the Botmaster, indicating its information (unique name, international mobile subscriber identity (IMSI), and IP address). Next, the Botmaster issues a command that instructs the infected devices to send bogus HTTP traffic to the victim Web server.

The generation of the bogus traffic is different from that of the genuine traffic since it relies on the considered traffic profile parameters. For example, for a mobile device to send HTTP traffic, a HTTP profile in the supported profile parameter for that device is identified (if any) and configured. Genuine HTTP traffic is generated by mobile devices that send HTTP traffic based on identified HTTP profiles whereas bogus HTTP traffic is generated when mobile devices that send HTTP traffic rely on no identified HTTP profiles; in this

case, the supported profile parameter value is set to *none*. Bogus traffic and genuine traffic are used to represent the DDoS attack traffic and the normal HTTP traffic, respectively. The normal HTTP traffic is generated as per the method provided in [54] using an average browsing packet size of 1608 bits and an average browsing inter-arrival time of 0.47 seconds. On the other hand, the DDoS attack traffic is generated as per the method provided in [55], using an inter-arrival time of 0.003 seconds.

In our simulations, the 500 mobile devices are configured with a profile parameter value of *none*, i.e. the traffic generated from them (via the execution process) are bogus ones. On the other hand, the 5 HTTP clients (i.e. legitimate customers) are configured to generate genuine HTTP traffic based on the normal HTTP traffic characterization. Both types of traffic are generated for 150 seconds, and a DDoS attack is created by overwhelming the victim Web server resources (i.e. CPU and bandwidth) with bogus HTTP requests over the LTE network. After starting the simulation time at time $t = 0$ seconds, the DDoS attack starts at a random time between $t = 100$ seconds and $t = 110$ seconds following these steps:

- *Phase 1*: At the start of the DDoS attack, a command is sent to all 500 mobile nodes in an attempt to infect them, and a notification report is sent back to the Botmaster indicating if the infection succeeded or did not.

- *Phase 2*: 150 seconds after the DDoS attack has started, at time $t = 250$ seconds, another command is sent that forces only the successfully infected mobile devices to start sending bogus HTTP traffic to the victim e-commerce Web server in an attempt to flood it.

The timeline of the DDoS attack model is depicted in Fig. 3.14 and Algorithm 1 is executed by the C&C server to launch the DDoS attack.

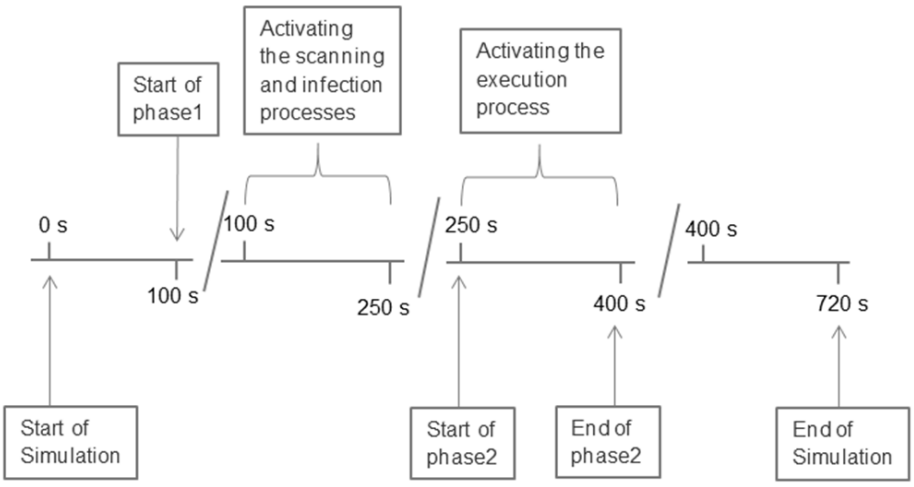


Figure 3.14: DDoS attack model timeline

Algorithm 1 Flooding algorithm run by the C&C server.

procedure FLOOD
  Input: N: number of vulnerable mobile nodes in the network.
  At time t = Random (100 seconds, 110 seconds)
  for each vulnerable node $i \in N$ **do**
    Inject the vulnerable nodes with the infection command.
    if infection is successful **then**
      confirmation messages will be sent to the Botmaster
    end if
  end for
  At time t = Random (250 seconds, 260 seconds)
  for each successfully infected node $j \in V$ where $V \subset N$ **do**
    sends an activation command to each $V(j)$ to start flooding the victim server.
  end for
end procedure

3.5 Performance Evaluation

3.5.1 The Riverbed Simulator

Riverbed simulator was formerly referred to as OPNET simulator. Riverbed simulator has an extensive set of network protocols and libraries, especially for wireless and cellular networks that consist of a suite of protocols such as VoIP, MPLS, IPv6, and different modules

of technologies such as WiMAX, UMTS, LTE. In this study, we have used the standard LTE module of Riverbed simulator. The LTE module of Riverbed simulator provides the capability of simulating a real LTE network based on the 3GPP standards [56] [57].

3.5.2 Simulation Results

The same LTE network parameters are applied to the two mobile botnet scenarios, SMM and AMM. The simulation parameters of both scenarios are configured as shown in Table 3.6. Also in this context, it should be noted that we have tried to run our simulation in more powerful computing environments such as using the facilities of Compute Canada to increase the simulation running time. But due to the licensing issues of the Riverbed simulator, that task was out of our control.

3.5.2.1 Number of infected devices

The number of infected mobile devices is varied between the SMM and AMM scenarios. This variation is the result of triggering a command of Phase 1 in the DDoS attack profile of the mobile botnet. The number of infected mobile devices through the duration of the DDoS attack is depicted in Fig. 3.15. In this figure, the first spike represents the overlapping of the number of infected mobile devices between the SMM and AMM scenarios at the beginning of Phase 1, which starts at time $t = 100$ seconds. The second spike represents the number of infected mobile devices of the AMM and SMM scenarios at the end of the simulation, which is at $t = 720$ seconds. Clearly, the number of infected mobile devices in the AMM scenario is higher than that obtained in the SMM scenario, where the number of the infected mobile devices in the AMM scenario is 380 mobile devices, and the number of the infected mobile devices in the SMM scenario is 300 mobile devices. Thus, using the AMM scenario yields a higher attack impact on the victim Web server compared to using the SMM scenario. It should be noted that the first spike represents the number of infected mobile devices during the activation of Phase 1 that spans from 100 to 250 seconds.

Table 3.6: Simulation parameters

Parameter	**Value**
Mobility Model	Random WayPoint, Shanghai taxi dataset
Wireless technology	LTE
Pathloss model	Free space
Cell Radius	1 km
UE Model	LTE mobile node
Number of UE nodes	500
Geographical overlay	Hexagon cell
UE Placement	Random way
Number of eNodeB stations	10
Number of EPC stations	1
Number of LTE cells	10
Simulation time	720 seconds
Mobility Start time	Start of simulation
Mobility Stop time	End of simulation
UE transmission power	0.005 watts
eNodeB transmission power	0.011 watts
Channel bandwidth	20 MHz
Duplex scheme	FDD

3.5.2.2 CPU Utilization

The relationship between the mobility models and the CPU resource consumption is investigated, revealing that there is a correlation between the movements' patterns of mobile users in the mobile botnet and the CPU performance as shown in Fig. 3.16. It can be observed that under the DDoS attack, the AMM scenario consumes more CPU resources than the SMM scenario. It should be noted that the massive increase in the CPU utilization of the victim web server that happens at time 250 seconds is interpreted due to the activation of the execution process that represents the initiation of the DDoS attack against the victim web server, which lasts for 150 seconds.

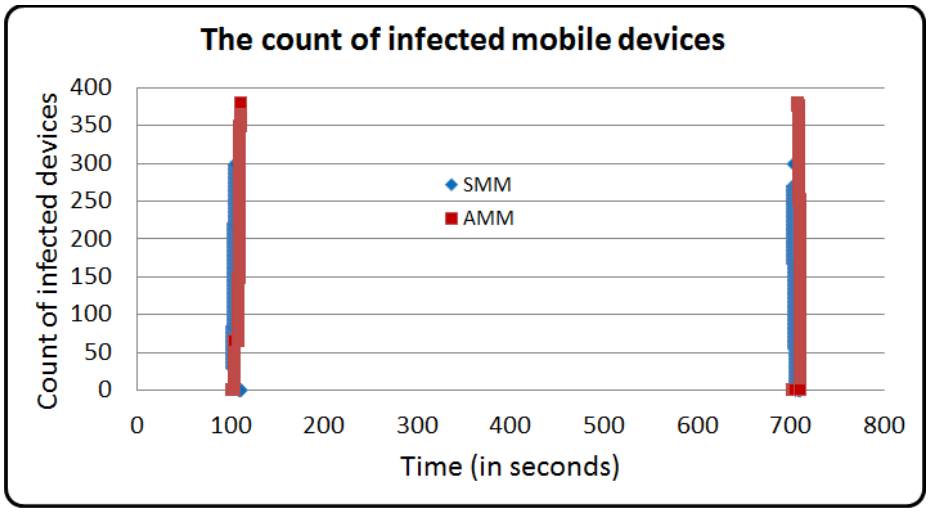


Figure 3.15: AMM scenario vs. SMM scenario in terms of the number of infected mobile devices

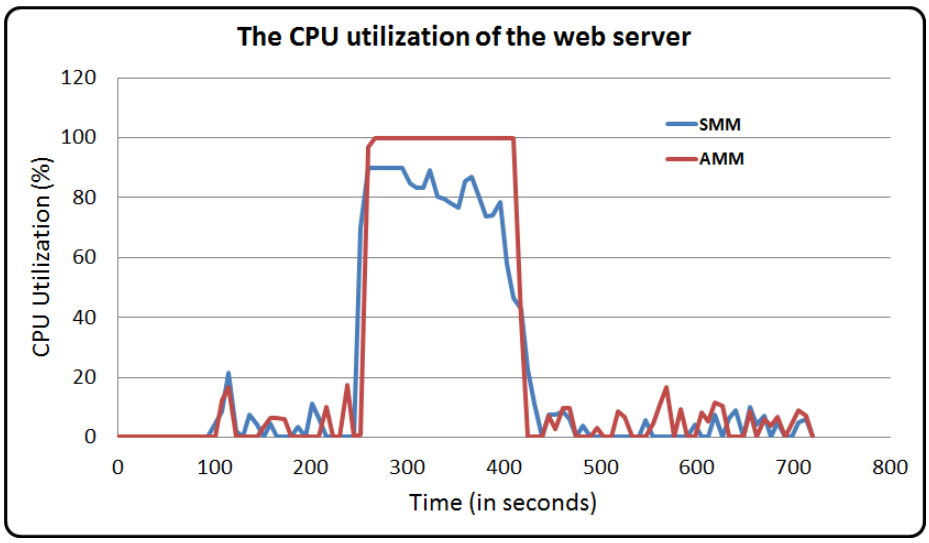


Figure 3.16: AMM scenario vs. SMM scenario in terms of CPU Utilization (%).

3.5.2.3 Task Processing Time

The task processing time consumed by the victim web server is investigated, which represents the time (in seconds) that was consumed by the victim Web server to process and respond to a request. The results are shown in Fig. 3.17. It can be observed that the AMM scenario consumes much more time than the SMM scenario, which is an indication that the probability of rejecting the legitimate HTTP requests in the AMM scenario is higher

than in the SMM scenario, i.e. the AMM scenario is more destructive compared to the SMM scenario. It should be noted that the huge increase in the task processing time of the victim web server that happens at time 250 seconds is interpreted due to the activation of the execution process that represents the initiation of the DDoS attack against the victim web server, which lasts for 150 seconds.

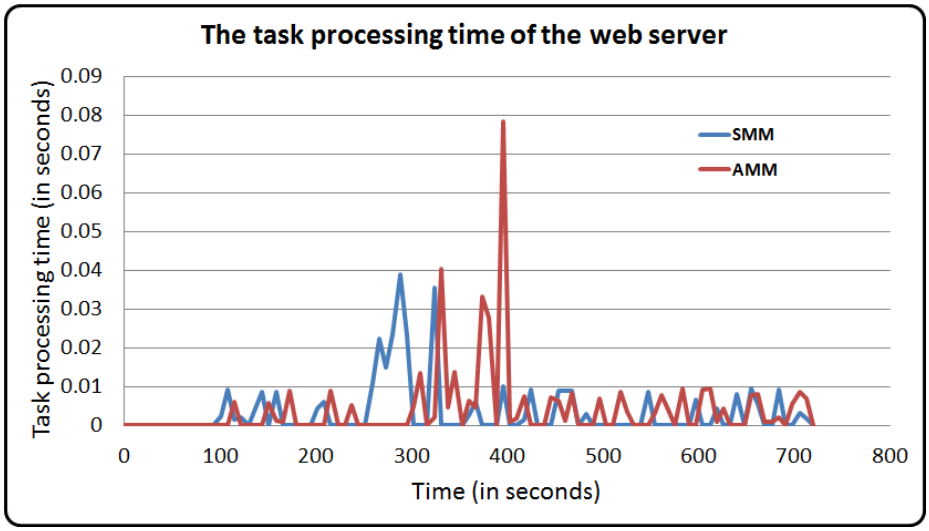


Figure 3.17: AMM scenario vs. SMM scenario in terms of task processing time in seconds

3.5.2.4 HTTP Load

The impact of the AMM and SMM mobility models on the Web server HTTP traffic load over time is investigated, where the HTTP load represents the rate at which the HTTP requests from different sessions arrive at the victim Web server. The results are shown in Fig. 3.18. It can be observed that the AMM scenario yields a much higher HTTP load than the SMM scenario does. It should be noted that the huge increase in the HTTP load of the victim web server that happens at time 250 seconds is interpreted due to the activation of the execution process that represents the initiation of the DDoS attack against the victim web server, which lasts for 150 seconds.

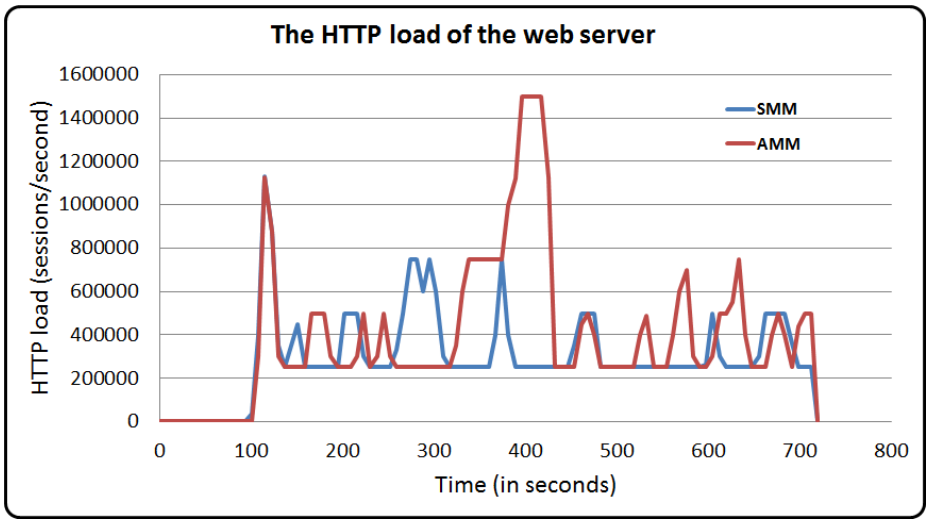


Figure 3.18: AMM scenario vs. SMM scenario in terms of HTTP load

3.5.2.5 HTML Object Response Time

The impact of the AMM and SMM mobility models on the response time of the legitimate requests is investigated. The results are shown in Fig. 3.19. It can be observed that the response time of the receiving HTML objects in the victim Web server in the AMM scenario is much higher compared to that generated by the SMM scenario during the DDoS attack. It should be noted that the huge increase in the HTML object response time of the legitimate clients that happens at time 250 seconds is interpreted due to the activation of the execution process that represents the initiation of the DDoS attack against the victim web server, which lasts for 150 seconds.

3.5.2.6 Uplink MAC Traffic Sent

The MAC traffic sent by the uplink level of the LTE network, i.e. the overall number of bits successfully transmitted by all the mobile devices in the LTE network toward the victim web server, is measured in order to evaluate the correlation between the SMM and AMM scenarios under the control of the mobile botnet as well as their impact on the LTE network behavior. The results are captured in Fig. 3.20. It can be observed that the number of bits

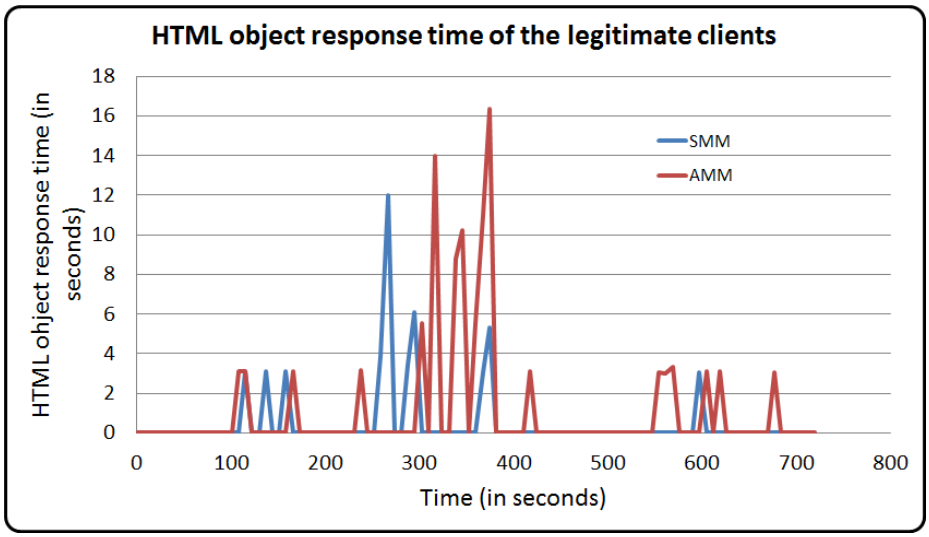


Figure 3.19: AMM scenario vs. SMM scenario in terms of HTML object response time

successfully transmitted to the victim web server is higher in the AMM scenario compared to that obtained in the SMM scenario in the presence of the DDoS attack. It should be noted that the massive increase in the LTE uplink MAC traffic sent that happens at time 250 seconds is interpreted due to the activation of the execution process that represents the initiation of the DDoS attack against the victim web server, which lasts for 150 seconds.

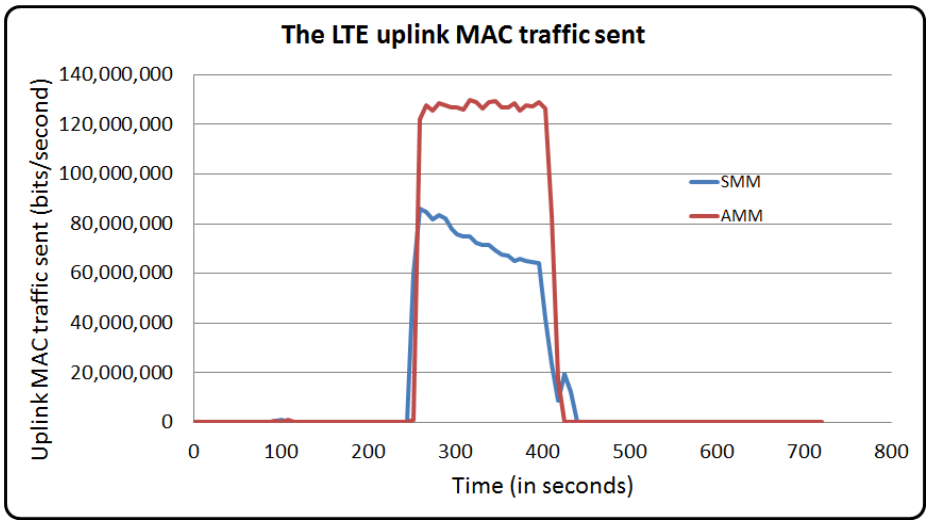


Figure 3.20: AMM scenario vs. SMM scenario in terms of Uplink MAC traffic sent

3.6 Summary

In this chapter, a mobile botnet that conducts a DDoS attack over a LTE network has been proposed. Our simulation results reveal that using the SMM model is advantageous compared to the AMM model in terms of (1) number of infected mobile devices, (2) CPU resource consumption, (3) task processing time consumed, (4) Web server HTTP traffic load over time, (5) receiving HTML objects, all in the victim Web server; and (6) the number of bits successfully transmitted to the victim Web server. This suggests that using the AMM model would yield a more severe threat impact of the mobile botnet on the victim Web server compared to using the SMM model. As a result, the SMM model can be used as a basis for an effective mitigation technique against the threats of mobile botnet networks. In this chapter we were able to set and define a relationship between the movements patterns (i.e. mobility dynamics) and the mobile botnet malicious operations over LTE network in terms of the number of infected mobile devices and the severity level impact on the victim server. The study revealed that the deployment of uniform movements patterns can mitigate the threat impact of a mobile botnet compared to the deployment of different random movements patterns.

The contribution in this chapter can be described in our ability to find a relationship between the mobility of mobile devices (AMM and SMM) and the threat impact of mobile botnets. We are the first researchers who were able to conduct and find this kind of correlation, where no one of the previous researchers did this kind of study.

Chapter 4

Impact of Base Transceiver Station Selection Mechanisms on Mobile Botnet

Understanding the behavior of a mobile botnet on a LTE network in the presence of DDoS attacks is still an open problem.

In this Chapter, we study the impact of two base transceiver station selection mechanisms, namely, the distance-based eNodeB (DBM) and the signal power-based eNodeB (SPBM) mechanisms, on a mobile botnet launching a DDoS attack on a LTE network involving 400 Android mobile devices. In the former mechanism, the selection of a suitable eNodeB station to serve the mobile devices' requests is based on the shortest distance metric whereas in the latter mechanism, the same selection is based on the strongest signal power.

4.1 LTE Infrastructure Cellular Network

The proposed mobile botnet is considered as an overlay network that operates over an LTE network as an infrastructure network, itself designed based on the 3GPP standards [44]. As per these standards, the LTE network architecture relies on the Evolved Packet System (EPS) architecture composed of user equipment (UE), evolved UMTS terrestrial radio access network (E-UTRAN), and Evolved Packet Core (EPC), all interconnected by means of three main interfaces, namely, Uu, S1, and SGi as shown in Fig. 4.1. Each of

these components consists of different stacks and levels as illustrated in Fig. 4.1, among which is the eNodeB stack. This stack represents the base transceiver station of the LTE network that supports the radio communication between the UE component and the other stacks of the EPC component.

The communication between an UE and the eNodeB is conducted through the Uu interface by sending and receiving the communication traffic (e.g., data and commands) using the uplink channels (UL) and downlink channels (DL). Every UE in the LTE network must be connected successfully to an eNodeB station (i.e. serving eNodeB) to be able to communicate and function in the cellular network. Two eNodeB stations can communicate with each other via the X2 interface, while the eNodeB can communicate with the MME stack and the SGW stack of the EPC component by using the S1-MME and S1-U interfaces, respectively.

The core structure of the EPC component is established by deploying four different stacks, which are:

- The Serving Gateway (SGW): this stack is responsible for managing the mechanism of routing and forwarding the data packets between the access network and the core network.

- The Packet Data Network Gateway (PGW): this stack represents the gateway that connects the core network of LTE with external Packet Data Networks (PDNs) such as the Internet via the SGi interface.

- The Mobility Management Entity (MME): this stack is responsible for controlling the security operation of mobile devices, mobility between 3GPP networks, EPS bearers regulation, and tracking location coordination.

- The Home Subscriber Server (HSS): this stack represents the subscribers database station of the LTE network where all their related information are saved.

As illustrated in Fig. 4.1, there is no direct communication path between mobile devices and the MME stack. Therefore, the LTE network was designed by integrating two layers of communication paths to manage the connection and transmission mechanism between the user equipment and the core network, namely, the Non-Access Stratum (NAS) layer and the Access Stratum (AS) layer. The NAS layer is deployed for transferring the signaling commands over the AS layer of the Uu and S1 interfaces.

The LTE network is an All-IP based system, which relies solely on the packet switching methodology as a communication domain. Therefore, each component of the EPS architecture is assigned an IP address to enable and facilitate the communication between these components over the underlying IP transport network.

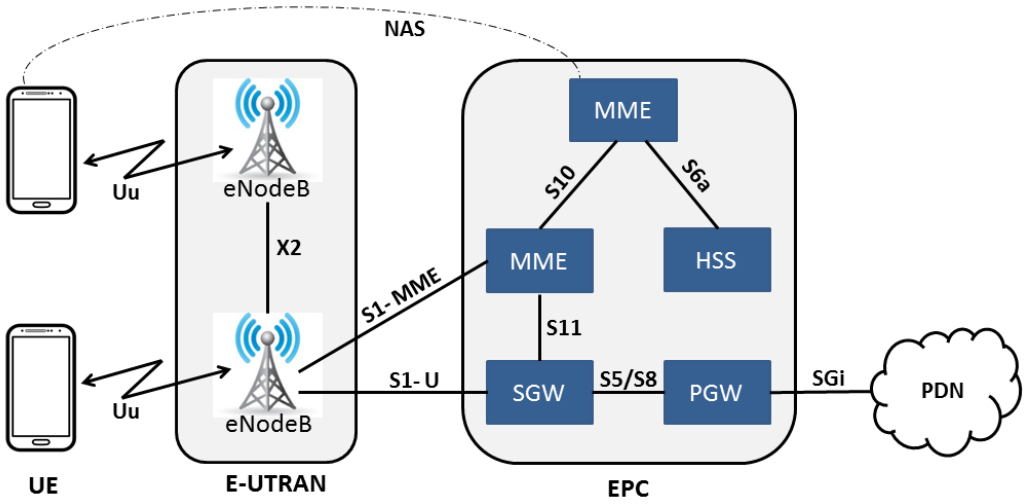


Figure 4.1: EPS architecture [2].

The proposed LTE network is deployed according to the LTE model implemented in the Riverbed Modeller [48], which follows the above 3GPP standards. The following parameters have been considered for the setup:

- Bearer: every mobile device is assigned two EPS bearers: the first one is the default bearer, which represents a non-guaranteed bit rate (Non-GBR) bearer that is used to manage the traffic connection between the HTTP application and the web server in the mobile botnet. The second bearer is the dedicated bearer, which represents a

guaranteed bit rate (GBR) bearer that is used to manage the video streaming application traffic of the web server as illustrated in Fig. 4.2. In this setting, two QoS Class Identifier (QCI) values are deployed, namely, QCI-2 and QCI-8 based on the standardized requirements of 3GPP TS 23.203 [44]. The QCI-2 value is meant to ensure the availability of the lowest quality required for the video application traffic, while the QCI-8 value is meant to ensure the best effort functionality of the traffic transmission.

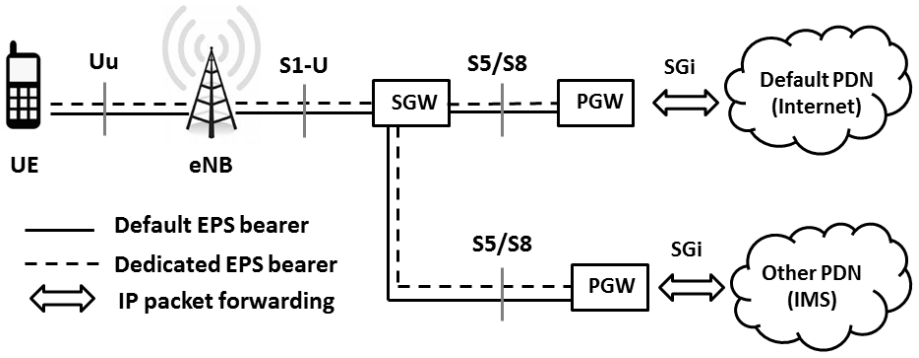


Figure 4.2: GBR and non-GBR EPS bearers of the considered LTE network.

The activation/deactivation mechanism of the EPS bearers is implemented according to the 3GPP standard [49]. Typically, a mobile device initiates an EPS bearer creation by dispatching an EPS session management (ESM) bearer resource modification request [49] to the EPC component of the core LTE network. When an EPS bearer is inactive, or an escalation request is triggered for a higher priority, an eNodeB station initiates the deactivation process of the EPS bearer. In addition, a GPRS Tunnelling Protocol (GTP) is implemented to handle the transfer of data from mobile devices to the web server on the Internet and vice-versa.

- Medium Access Control (MAC): a MAC layer is deployed to map the EPS bearers into logical channels, and to map these logical channels into transport channels as shown in Table 4.1. Typically, a mobile device activates the random access procedure of the MAC layer to send Common Control Channel (CCCH) messages to the

eNodeB in order to complete the Radio Resource Control (RRC) connection setup during the network attachment process [44].

Table 4.1: Mapping of Logical channels to Transport channels

Direction	**Logical channel**	**Transport channel**	**Usage**
Downlink	CCCH	Downlink shared channel	Control messages sent before UE RRC connection
	Dedicated traffic channel		Downlink user data
	Dedicated control channel		Downlink control information
Uplink	CCCH	Uplink shared channel	Control messages sent before RRC connection
	Dedicated traffic channel		Uplink user data
	Dedicated control channel		Uplink control information

- Admission Control Procedure: this procedure is implemented by each eNodeB station in the LTE network to serve its cell. Any request for a GBR radio bearer from the eNodeB station should go through this procedure. When a GBR radio bearer request is established, this procedure allocates and reserves the required cell resources for a GBR bearer. When the GBR radio bearer is deactivated, the same procedure releases the allocated cell resources, returning it back to the pool of available cell resources. A GBR radio bearer is admitted only if the required cell resources are available and

can be allocated to the uplink and downlink directions. Otherwise, the request will be rejected. In our settings, the preemption procedure of the admission control is enabled, by using the Allocation and Retention Priority (ARP) parameter. Indeed, the priority level of a GBR radio bearer is determined based on its ARP value, which is represented by an integer from the range 1 to 15. Low ARP values correspond to high priority levels, whereas high ARP values correspond to low priority levels. In our settings, the ARP parameter is constant and set to the default value since only one GBR radio bearer is considered.

- Mobile device's control mechanism: each mobile device is controlled by two entities as shown in Fig. 4.3: (1) the eNodeB stack through signaling messages that are written by using the RRC protocol, and (2) the Mobility Management Entity (MME) stack through some signaling messages written by using the EPS mobility management (EMM) protocol [44]. A mobile device can switch from one EMM state to another when certain conditions occur, as described in Table 4.2. For instance, when a tracking area update is needed or when there is traffic that should be delivered from/to the core network.

- Physical layer deployment: this works in both the Frequency Division Duplex (FDD) and the Time Division Duplex (TDD) modes [44]. In our settings, a resource block (RB) is composed of 84 resource elements, by combining one 0.5 ms time slot and 12 sub-carriers, each of which has 15 KHz. Typically, each frame in the scheduler is subdivided into multiple subframes of 1 ms length units each. In addition, the FDD duplex system uses the Type-1 frame structure and the channel bandwidth is configured to operate with 20 MHz using 100 as the number of resource blocks [44]. The base frequency is set to 1920 MHz for the uplink channel and 2110 MHz for the downlink channel, and six physical channels are considered as described in Table 4.3.

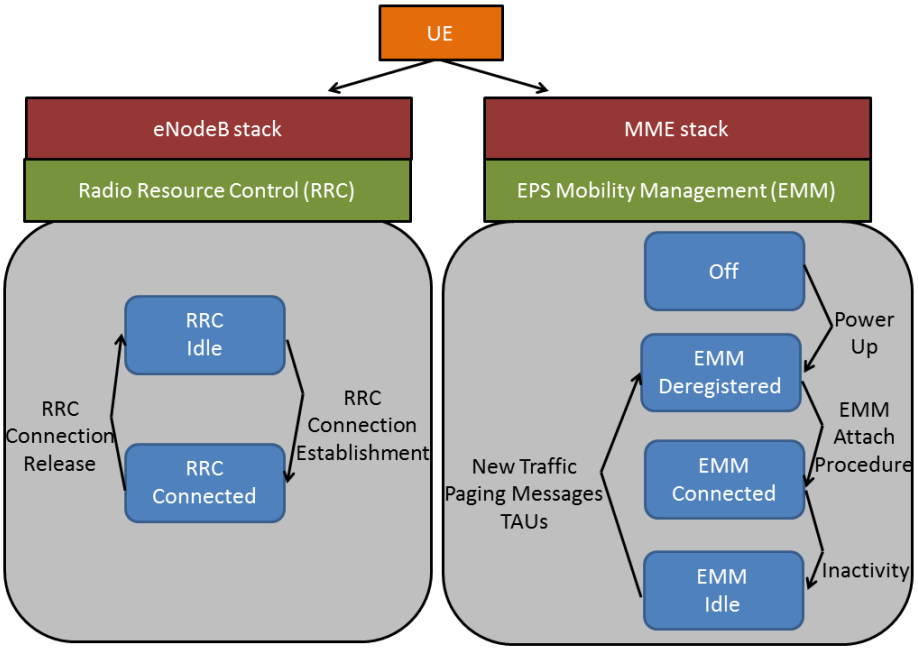


Figure 4.3: Mobile device control mechanism [46].

Table 4.2: Mobile device's EMM states

EMM State	**Role**
Off	When a mobile device is turned off and there is no activity or connection with the core network
EMM_Deregistered	When a mobile device starts the EMM Attach procedure with the core network or awaits for completing this procedure.
EMM_Connected	When a mobile device completes the attachment procedure successfully and is registered with the core network [49].
EMM_Idle	When a mobile device has no activity in the LTE network and cannot save a considerable amount of its power.

Table 4.3: Types of physical channels.

Physical channel	**Functions**
Primary broadcast channel	To transfer the primary and secondary synchronization signals, and the master information block messages.
Physical downlink shared channel	To send the downlink data and the system information block messages.
Physical downlink control channel	To transfer the downlink control information, RAR, and CCCH messages.
Physical random access channel	To deliver the random access preambles of the random access procedure. To prevent a collision between different preambles, the contention random access procedure is invoked.
Physical uplink shared channel	To transmit the uplink data traffic.
Physical uplink control channel	To transmit the uplink control traffic.

4.2 Base Transceiver Station Selection Modes

In order for a UE (i.e. mobile device) to access the LTE network services and facilities, a Base Transceiver Station (BTS) such as an eNodeB station (referred to as serving eNodeB) must be selected and the UE must be connected to it. In this chapter, the impact of two eNodeB selection mechanisms on the attack severity of the proposed mobile botnet on the considered LTE network is assessed, namely, the distance-based mode (DBM) and the signal power based mode (SPBM). Our experiments involving designing the two BTS selection modes (DBM and SPBM) reveal a solid relationship between these two modes and the malware propagation mechanism, which affects the attack severity level of a mobile botnet. We present these two selection mechanisms in the following subsections.

4.2.1 Distance-Based Model Mode

In this mode, the selection of the serving eNodeB station relies on the distance measure between the mobile device and the available eNodeB stations. In our settings, the Reference Signal Received Power (RSRP) and the Maximum Transmission Power (MTP) attributes of the eNodeB stations are configured in the E-UTRAN component of the LTE network in such a way that each eNodeB station can serve multiple mobile devices and each mobile device can conduct the cell search and selection process by registering with a candidate EPC node during the EMM attachment procedure [49]. The eNodeB station that has the shortest distance to the UE among all other eNodeB stations is chosen as serving eNodeB. Typically, at the start of the simulation, each mobile device attempts to register with an EPC node in the core LTE network via the EMM attachment procedure. Afterwards, every 240 ms, a mobile device sends a report to its encountered eNodeB station, which includes a list of eNodeB stations managed by the serving EPC component and their related distance measures. If the encountered eNodeB station detects a distance measure shorter than its own, it will decide to handover the mobile device to that shorter distance eNodeB station,

now considered as its newly serving eNodeB station. During this process, the handover procedure is initiated by sending a handover request from the current encountered eNodeB station to the newly selected one. If the latter station accepts the bearer of the mobile device, a notification message is sent back to the current encountered eNodeB station to confirm the acceptance of the mobile device. In its turn, this eNodeB station sends a handover command message to the mobile device to transfer the data packets to the newly selected eNodeB station. The handover procedure is configured as X2-handover by default if the X2 interface is available. Otherwise, it is configured as a S1-handover through the S1 interface.

4.2.2 Signal Power Based Model Mode

In this mode, the signal strength of the eNodeB station is used as the selection criterion. In our settings, the RSRP (Reference Signal Received Power) is used to measure the total received power in the LTE network. The process of selecting a suitable LTE cell is conducted during the EMM attachment mechanism [49] as done in the DBM mode. When an EPC station is successfully selected, the mobile device selects a suitable cell by checking the frequencies of all the eNodeB stations of its serving EPC. In doing so, the received power (P_R) is determined by using the equation:

$$P_R = T_t \times N_t \times \left(\frac{W^2}{16\Pi^2 d^2} \right) \times N_r \tag{4.1}$$

where T is the transmission power, N is the antenna gain, d is the distance between the source-destination node pair, t represents the radio transmitter, r represents the radio receiver, and W is the signal wavelength. It should be noted that every eNodeB station in the LTE network is assigned a MTP value (measured in watts W) as shown in Table 4.4.

At the start of the simulation, each mobile device attempts to register with an EPC node in the core LTE network via the EMM attachment procedure. Afterward, each UE starts to scan all the eNodeB stations in the network to find a suitable eNodeB station to be

connected to, based on the signal power strength criterion.

Table 4.4: MTP values of the eNodeB stations.

eNodeB station	**MTP value** (W)	**eNodeB station**	**MTP value** (W)
eNB1	0.011	eNB11	0.011
eNB2	0.031	eNB12	0.031
eNB3	0.051	eNB13	0.051
eNB4	0.071	eNB14	0.071
eNB5	0.091	eNB15	0.091
eNB6	0.111	eNB16	0.111
eNB7	0.131	eNB17	0.131
eNB8	0.151	eNB18	0.151
eNB9	0.171	eNB19	0.171
eNB10	0.191	eNB20	0.191

In the SPBM mode, the eNodeB station is responsible for triggering and managing the handover procedure as described in [49]. Typically, periodic reports are generated by each mobile device and sent to all eNodeB stations in the network every 200 ms. The handover procedure is initiated when the current serving eNodeB station receives a periodic report that contains a RSRP value higher than its own RSRP value. In this case, the current serving eNodeB station triggers a X2-handover procedure with the newly discovered eNodeB station if the X2 interface is available. Otherwise, a S1-handover is initiated through the S1 interface. In turn, the new serving eNodeB station sends a handover command message to the mobile device allowing the device to transfer its data packets to its intention.
The difference between the DBM and SPBM modes is illustrated in Fig. 4.4, where 4 eNodeB stations are considered, namely, eNB1, eNB2, eNB3, and eNB4, each having its own signal power strength measured in β units.

In Fig. 4.4, the green mobile node is moving around a specific region following the red dashed trajectory path. At time $t = 3$ seconds, the mobile node will be connected to eNB1 in the DBM mode and to eNB2 in the SPBM mode. After 20 seconds, at time $t = 23$

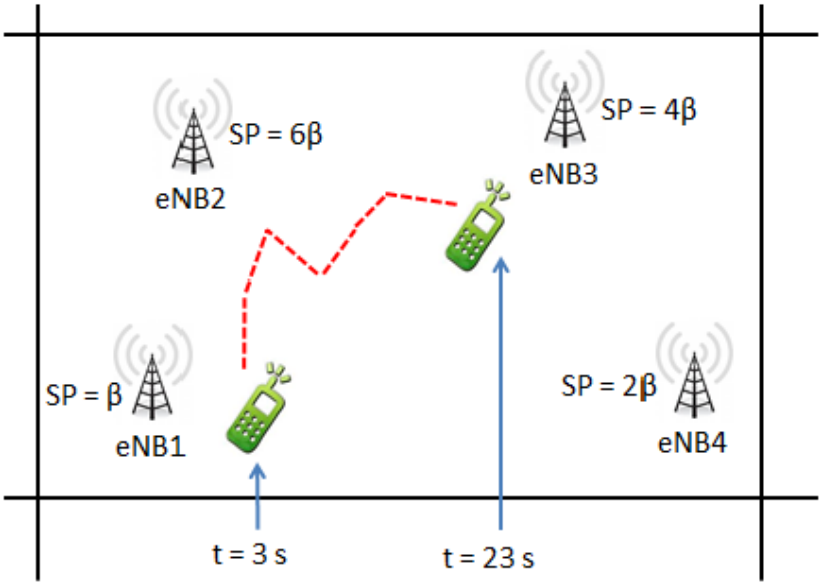


Figure 4.4: DBM vs. SPBM

seconds, the mobile node will be connected to eNB3 in the DBM mode and to eNB2 in the SPBM mode.

4.3 Mobile Botnet Topology and Attack Model

The considered mobile botnet architecture is composed of a botmaster, the C&C server, and the LTE network as shown in Fig. 4.5.

The botmaster is responsible for managing all the mobile botnet operations by controlling the C&C server. This server is used as a gateway for the botmaster to access the infected mobile devices and deliver malicious commands using the push method. In this experiment, the LTE infrastructure network is made of 20 hexagon cells, each of which has a 1 km radius, a 20 MHz channel bandwidth, and 20 mobile devices controlled by a single eNodeB station. An EPC node is used which communicates with the 20 eNodeB stations in the E-UTRAN component.

Two simulation scenarios are considered. In the first scenario, 400 mobile devices in

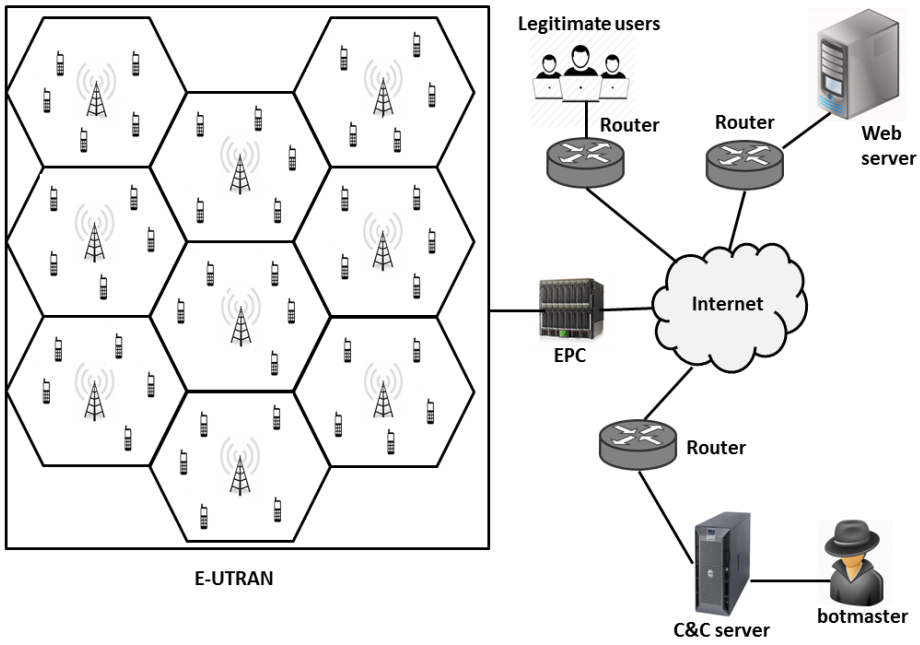


Figure 4.5: Mobile botnet architecture.

the LTE network are allowed to be connected to their serving eNodeB stations based on the DBM mode. While in the second scenario, the 400 mobile devices in the LTE network are allowed to be connected to their serving eNodeB stations based on the SPBM mode.
The functionality of the mobile botnet is executed through four main stages as per Table 4.5.

The trajectories of the movement of the mobile devices are simulated by using the Random WayPoint (RWP) model, which is a segment-based trajectory model. The deployed RWP model could be described as a stochastic model, where a mobile device selects randomly a destination point e in the deployment network K. Every mobile device follows its trajectory path by using a selected random speed s, where $0 < s < \infty$. Upon the arrival of a mobile device to its destination point, it waits for a suspension time m, before moving to a new random destination point. Therefore, the stochastic process of the RWP model of each mobile device can be expressed as $\{(E_1, M_1, S_1), \ldots, (E_i, M_i, S_i), \ldots\}$, where E_i denotes a destination point in K, M_i represents the suspension time in the destination point E_i, and S_i represents the speed of the mobile device during the discrete time i.

Table 4.5: Functionality of the mobile botnet

Function	**Performed by**
Reconnaissance	scanning the mobile devices in the LTE network in order to identify the vulnerable ones.
Propagation	sending a malware command to all the identified vulnerable mobile devices, with the goal to infect the maximum number of devices.
Notification	forwarding a report that indicates the information about the successfully infected mobile devices to the botmaster.
Swamping	by executing a DDoS attack against the victim e-commerce web server.

All destination points E_i are distributed arbitrarily by a uniform distribution over the deployment network K, excluding E_0, which is created by the initial spatial function $f_{spatial}(x)$ of the mobile devices. The function $f_{spatial}(x)$ identifies randomly the initial spatial placement point of each mobile device in the LTE network at the beginning of the simulation setup. The movement from e_{i-1} to e_i represents a single fragment (F_i) in the trajectory path of a mobile device. Therefore, combining all the fragments generates the entire trajectory path of a mobile device, which is represented by $\{F_1, \ldots, F_i, \ldots\} = \{e_1 - e_0, \ldots, e_i - e_{i-1}, \ldots\}$.

The deployment network K is implemented as the shape of a rectangle, which is identified by using four attributes, namely, K_{west} which represents the west boundary limit of the rectangular area K, K_{east} which represents the east boundary limit of the rectangular area K, K_{south} which represents the south boundary limit of the rectangular area K, and K_{north} which represents the south boundary limit of the rectangular area K.

At the start of the simulation, the RWP profile configuration is deployed in each mo-

bile device in the LTE network. Then, each mobile device moves according to its trajectory fragments from one destination point e_i to the next destination point e_{i+1}. The considered RWP profile configuration attributes are given in Table 4.6

Table 4.6: RWP profile configuration

Parameter	**Value**
K_{west}	-4,000 meters
K_{east}	5,500 meters
K_{south}	-4,330.127 meters
K_{north}	4,330.127 meters
S	5 meters/second
M	100 seconds

A sample of a RWP trajectory path that is made up of 8 fragments $\{F_1, \ldots, F_8\}$ is shown in Fig. 4.6.

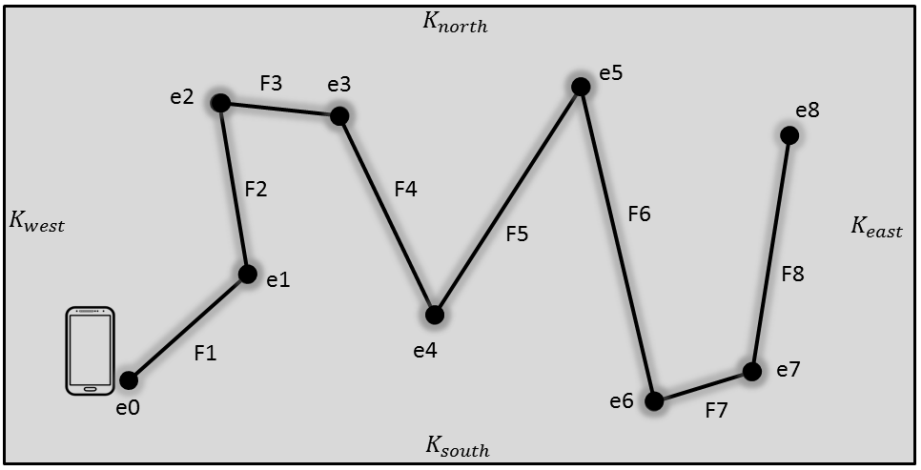


Figure 4.6: Sample of RWP trajectory path

A DDoS attack scenario is triggered by the botnet C&C server by inspecting the 400 mobile devices in the LTE network. Once the inspection process is completed and the vulnerable mobile devices are identified, a malware command is sent by the C&C server to perform the trojan malware installation operation by using a re-packaging, update-attack, or drive-by-download technique [53]. A report is then sent to the botmaster, providing

some information related to the successfully infected mobile devices (e.g. device's name, cell number, MAC address). Next, a command is sent by the botmaster through the C&C server to all the infected mobile devices to initiate a DDoS attack (i.e. fake HTTP requests are sent to the victim web server). In this process, real HTTP traffic is generated only when the HTTP profile of the mobile device in the traffic generation module of the Riverbed Modeller [48] can be identified and its parameter has been set to the value *activate*. On the other hand, fake HTTP traffic is generated from a mobile device when the HTTP profile parameter of that device has been set to the value *deactivate*. For real traffic, the packet size and inter-arrival time parameters have been set to 201 bytes and 470 milliseconds, respectively. For fake traffic, the traffic characteristics are inherited from [55], considering an inter-arrival time of 3 milliseconds. The DDoS attack model against the victim web server is shown in Fig. 4.7.

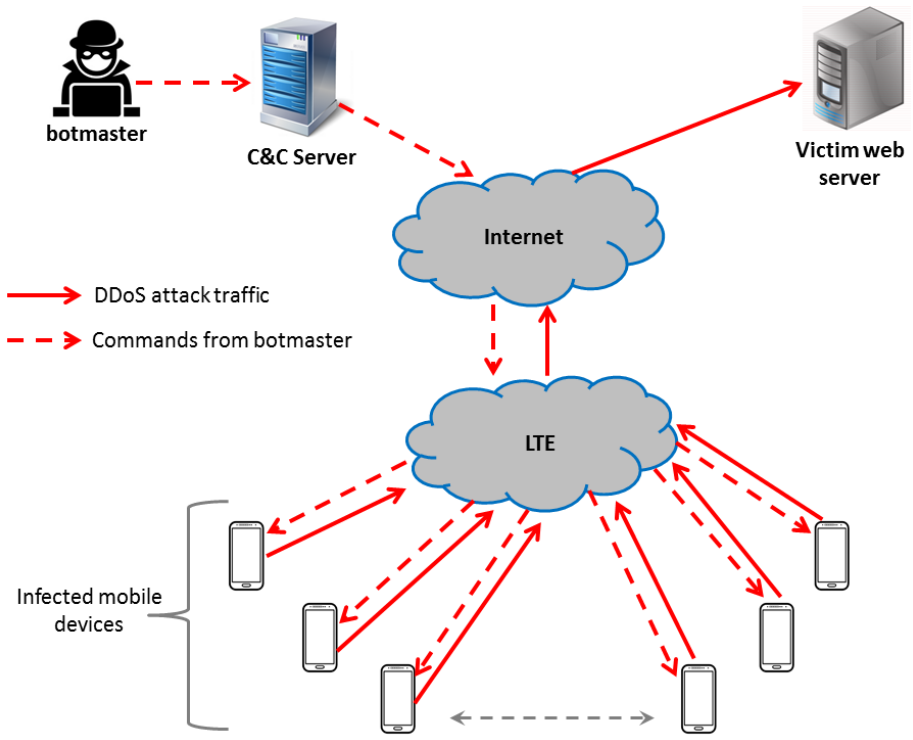


Figure 4.7: DDoS attack model.

To implement the DDoS attack, all the 400 mobile devices in the LTE network are

configured using the HTTP profile parameter value *deactivate*. In addition, 5 HTTP workstations are configured using the HTTP profile parameter value *activate*. These represent the legitimate users who have access to the web site on the victim web server. Launching the DDoS attack leads to flooding the resources of the victim web server such as CPU and bandwidth. The generation of the attack traffic is triggered over two phases. Phase 1 represents the beginning of triggering the DDoS attack, initiated by sending a command from the botmaster through the C&C server to infect the maximum possible number of mobile devices in the LTE network. As a result of a successful infection, a notification is sent to the botmaster. Phase 2 starts at time $t = 250$ seconds by sending a command from the botmaster through the C&C server to all the infected mobile devices in the LTE network, which initiates the DDoS attack against the victim web server. The timeline of the DDoS attack model is depicted in Fig. 4.8.

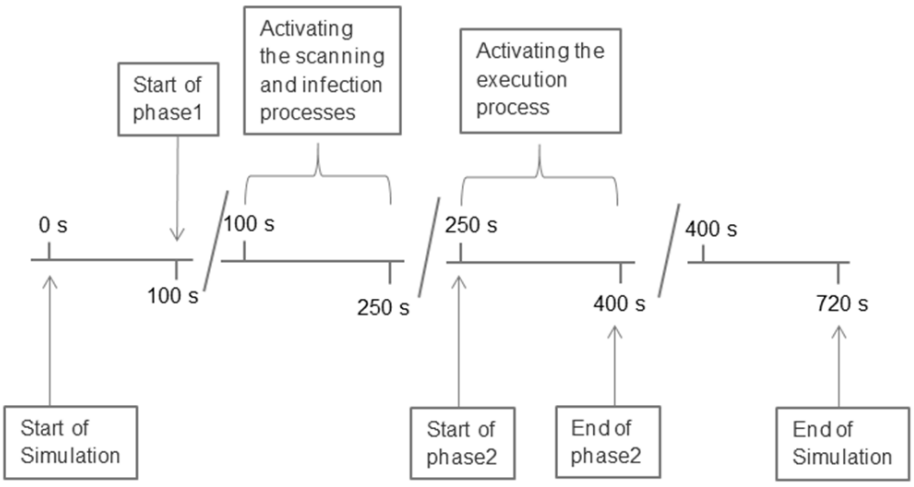


Figure 4.8: DDoS attack timeline

4.4 Performance Evaluation

For the considered DBM and SPBM scenarios, the same LTE network configuration features given in Table 4.7 are considered.

Table 4.7: Simulation Attributes

Parameter	**Value**
Mobility model	RandomWayPoint
Wireless technology	LTE
Path loss model	Free space
Cell radius	1 km
UE model	LTE mobile node
Number of UE nodes	400
Geographical overlay	Hexagon cell
UE placement	Random fashion
Number of eNodeB stations	20
Number of EPC stations	1
Number of LTE cells	20
Simulation time	720 seconds
Mobility start time	Start of simulation
Mobility stop time	End of simulation
Channel bandwidth	20 MHz
Duplex scheme	FDD

4.4.1 Simulation Results

4.4.1.1 Number of infected mobile devices

The number of infected mobile devices is investigated when using the DBM vs. the SPBM scenarios. The results are summarized in Fig. 4.9, which depicts the difference in the number of infected devices at the start of the DDoS attack at time $t = 100$ seconds and at the end of the DDoS attack at time $t = 720$ seconds. It is observed that the number of successfully infected mobile devices is 340 in the DBM scenario and 290 in the SPBM scenario. This difference is attributed to the implementation of the stage A of the DDoS attack model, by initiating the botmaster command that attempts to infect the maximum possible number of mobile devices in the LTE network. Clearly, the attack severity of the

mobile botnet on the victim web server is more pronounced when using the DBM model compared to the SPBM model. It should be noted that the first spike represents the number of infected mobile devices during the activation of Phase 1 that spans from 100 to 250 seconds.

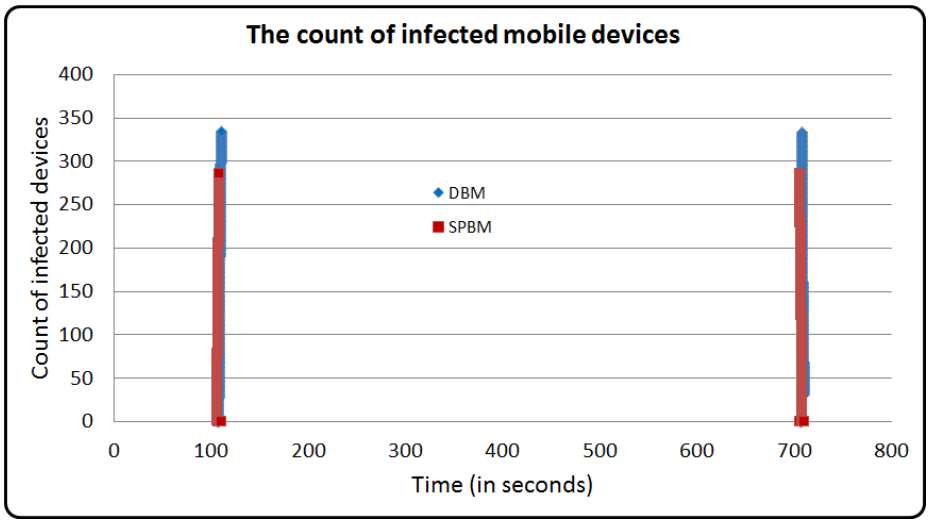


Figure 4.9: Number of infected mobile devices when for DBM vs. SPBM.

4.4.1.2 CPU Utilization

The CPU utilization of the victim web server is measured when using the DBM vs. the SPBM scenarios. The results are captured in Fig. 4.10, showing that the process of deploying the DBM mode leads to higher CPU utilization of the victim server compared to when the SPBM is used, which is also an indication of the above-mentioned higher attack severity when using the DBM scenario. It should be noted that the massive increase in the CPU utilization of the victim web server that happens at time 250 seconds is interpreted due to the activation of the execution process that represents the initiation of the DDoS attack against the victim web server, which lasts for 150 seconds.

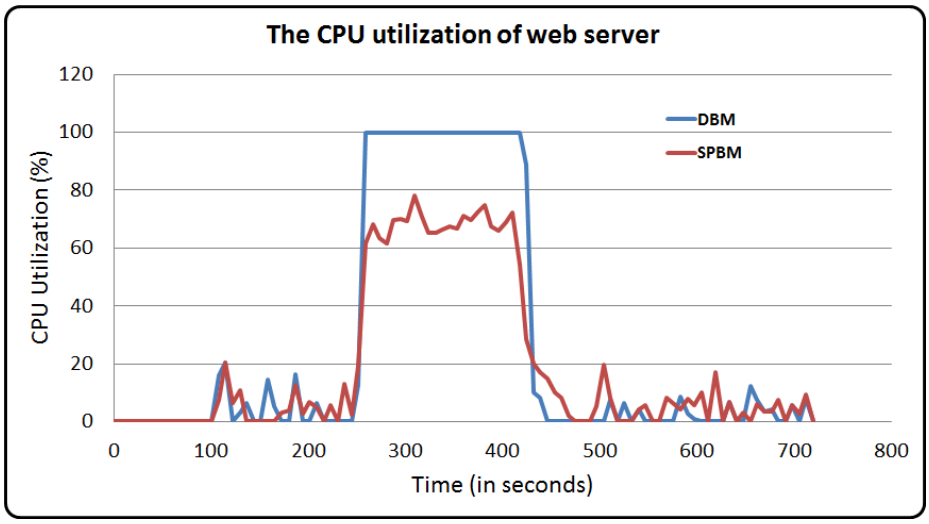


Figure 4.10: CPU utilization for DBM vs. SPBM.

4.4.1.3 LTE Uplink MAC Traffic

Fig. 4.11 depicts the total amount of uplink MAC traffic sent by all mobile devices in the LTE network, i.e. the overall number of bits successfully transmitted by these devices toward the victim web server. It is observed that this number is very high when using DBM compared to SPBM. It should be noted that the massive increase in the LTE uplink MAC traffic that happens at time 250 seconds is interpreted due to the activation of the execution process that represents the initiation of the DDoS attack against the victim web server, which lasts for 150 seconds.

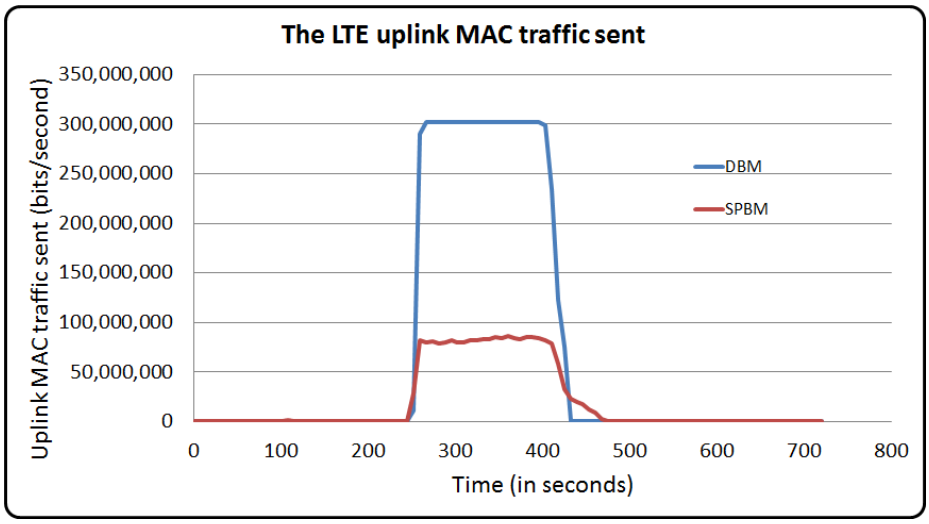


Figure 4.11: LTE uplink MAC traffic for DBM vs. SPBM.

4.4.1.4 Uplink Throughput

Fig. 4.12 captures the uplink throughput of all eNodeB stations in the LTE network when using DBM compared to using SPBM. It is observed that the uplink throughput of the eNodeB stations under the DDoS attack is much higher when using DBM compared to using SPBM. It should be noted that the massive increase in the uplink throughput that happens at time 250 seconds is interpreted due to the activation of the execution process that represents the initiation of the DDoS attack against the victim web server, which lasts for 150 seconds.

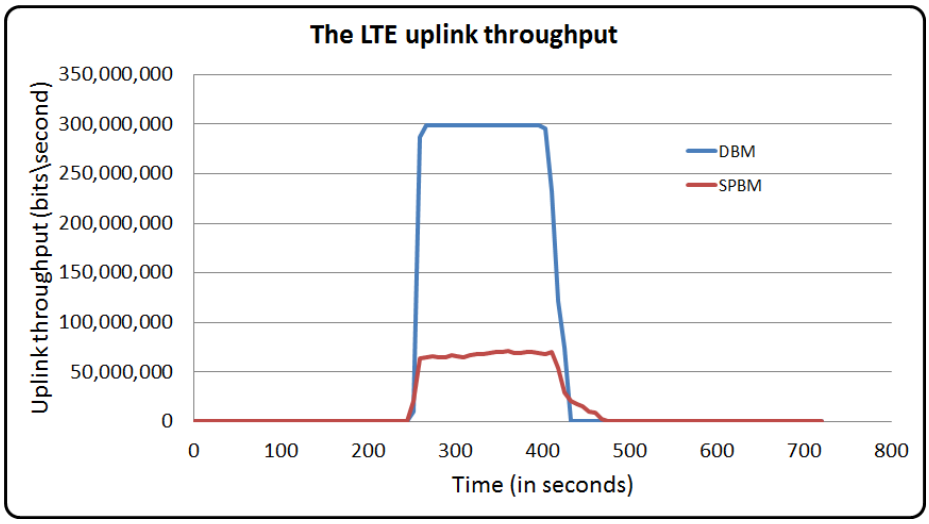


Figure 4.12: Uplink throughput for DBM vs. SPBM.

4.4.1.5 HTTP Traffic Load

The HTTP load consumed over time by the victim web server is investigated for DBM vs. SPBM. This metric represents the rate of HTTP requests from different sessions arriving at the victim web server. The results are captured in Fig. 4.13. It is observed that the DBM scenario consumes a higher load on the victim web server compared to the SPBM scenario. It should be noted that the huge increase in the HTTP traffic load of the victim web server that happens at time 250 seconds is interpreted due to the activation of the execution process that represents the initiation of the DDoS attack against the victim web server, which lasts for 150 seconds.

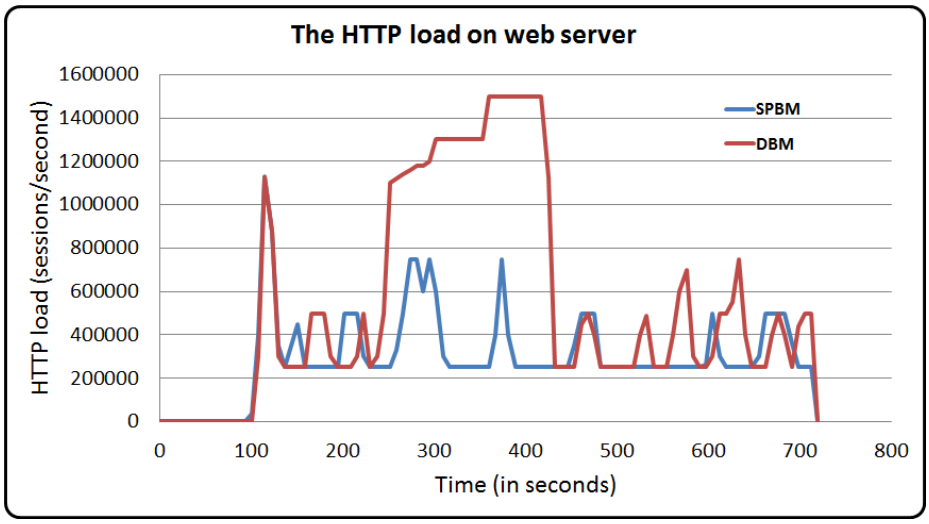


Figure 4.13: HTTP traffic load for DBM vs. SPBM.

4.5 Summary

This Chapter has proposed a mobile botnet model that launches a DDoS attack against a victim web server. The impact of two base transceiver station selection mechanisms, namely, DBM and SPBM on the proposed mobile botnet is investigated by simulations. The simulations show that the DBM mechanism yields a higher threat impact on the victim server compared to the SPBM mechanism, in terms of (1) total number of infected mobile devices, (2) consumed CPU resource, (3) total amount of uplink MAC traffic sent by all mobile devices, (4) Uplink throughput of all eNodeB stations, and (5) HTTP traffic load consumed by the victim server over time. The results of this study could be used as a basis for developing an efficient mitigation technique against the threats of mobile botnets.

In this chapter we were able to set and define a relationship between the process of selecting an eNodeB station in LTE network and the mobile botnet malicious operations in terms of the number of infected mobile devices and the severity level impact on the victim server. The study revealed that the mechanism of choosing an eNodeB station based on the RSRP strength value only can reduce and mitigate the threat impact of a mobile botnet compared

to the mechanism of choosing an eNodeB station based on the distance factor only.

The contribution in this chapter can be described in our ability to find a relationship between the eNodeB stations selection mechanisms (DBM and SPBM) and the threat impact of mobile botnets. We are the first researchers who were able to conduct and find this kind of correlation, where no one of the previous researchers did this kind of study.

Chapter 5

Epidemic SMS-based Cellular Botnet

Attacks and threats against cellular devices such as botnets are becoming more and more prominent. Focusing on short message services (SMS) phishing attacks, this Chapter investigates the design of a cellular botnet that initiates such attack and studies its epidemic behavior using three random graphs models, namely the Barabasi–and-Albert topology (BAT), Erdos-and-Reyni topology (ERT), and Watts-and-Strogatz topology (WST).

5.1 Considered Approach

A cellular botnet network relies on the C&C channel, which represents its core component. That channel should have two epidemic characteristics, namely speed and stealth. The speed characteristic refers to the ability of the botmaster through the C&C channel to propagate the malware to a vast amount of susceptible cellular devices in a short time. On the other hand, the stealth characteristic refers to the ability of disseminating the malware in a concealed manner so that the cellular users cannot detect the malware propagation mechanism. Therefore, in this Chapter, we have considered those characteristics in designing the proposed epidemic cellular botnet.

The architecture of our proposed cellular botnet is implemented by leveraging the SMS mechanism as a C&C channel, which is a low cost service available in all cellular phone

devices. In doing so, there is a dilemma that had to be solved, that is the tradeoff between propagating rapidly the malicious commands to a large number of susceptible cellular phone devices in the network and deploying a stealthy C&C channel. In other words, for a botmaster to be able to disseminate the malicious SMS to a large number of susceptible cellular devices in a short period of time, a group-messaging mechanism must be applied, which contradicts the concept of a stealthy C&C channel because a group-messaging mechanism facilitates the detection of the malicious SMS and C&C channel behavior by end users. Therefore, the main challenge in our design is to decide on how to deploy the C&C channel that can quickly disseminate malicious SMS messages to a large number of cellular devices while satisfying the stealth characteristic?

We have studied and evaluated the epidemic behavior of the proposed cellular botnet by deploying a command and control (C&C) mechanism that relies on an epidemic flooding algorithm. The following topologies have been implemented to study their impact on the behavior and operations of the proposed epidemic cellular botnet, namely, the Barabasi–and-Albert topology (BAT), the Erdos-and-Reyni topology (ERT), and the Watts-and-Strogatz topology (WST). Also, two cdevice failure paradigms have been implemented, namely, the selective cdevice failure, and the random cdevice failure, with the goal to measure the resilience of the proposed cellular botnet against the failure of the infected cellular devices.

5.2 Epidemic Command and Control Mechanism

5.2.1 Epidemic Flooding Algorithm

In our proposed epidemic cellular botnet, we have chosen the SMS mechanism as a C&C channel, due to the following reasons:

- Available statistics indicate that the successful open rate of SMS is more than 98%. And out of this 98% rate, 90% of the open rate occurs within 3 minutes of receiving

the SMS messages by end users [58].

- SMS service doesn't rely on the Internet as a transmission medium, which makes it an omnipresent mechanism. Omnipresence means that the SMS could reach end users everywhere, and at any time of the day.

- The SMS service is available almost in all the cellular phone devices, i.e. in the new generation cellular devices (i.e. smart-phones), and in the old generation cellular devices. In addition, the SMS service is available on all the platforms (e.g. Android, and iOS).

- SMS is a simple and robust text messaging mechanism; just having a cellular phone number is enough to send the SMS message to a susceptible cellular device, with almost zero error rate.

Therefore, choosing the SMS mechanism as a C&C channel to support the epidemic behavior of our cellular botnet network is appealing. Besides, the SMS mechanism is an efficient and practical method that lures the attackers (e.g. botmaster) to leverage it as a mechanism to be considered in their cellular botnet networks.
Our proposed epidemic SMS-based cellular botnet consists of the botmaster, C&C server (or seed), C&C channel that leverages the SMS mechanism, C&C messages - which represent the malicious commands sent by the botmaster, and susceptible cellular phone devices (cdevices), as depicted in Fig. 5.1.

In our proposed cellular botnet (Fig. 5.1), there are 2000 susceptible cdevices, each of which has 6 peers on average, and the C&C server (i.e. the seed, here represented by $K1$) is selected as the hub cdevice i.e. the cdevice with the highest number of directly connected peers in the network. Prior to activating the botnet, a verification process is launched for all cdevices to evaluate their degrees, and then the hub is selected.

Once $K1$ has been identified, the communication starts between the botmaster and the susceptible cdevices via the hub cdevice. If the botmaster decides to send a malicious

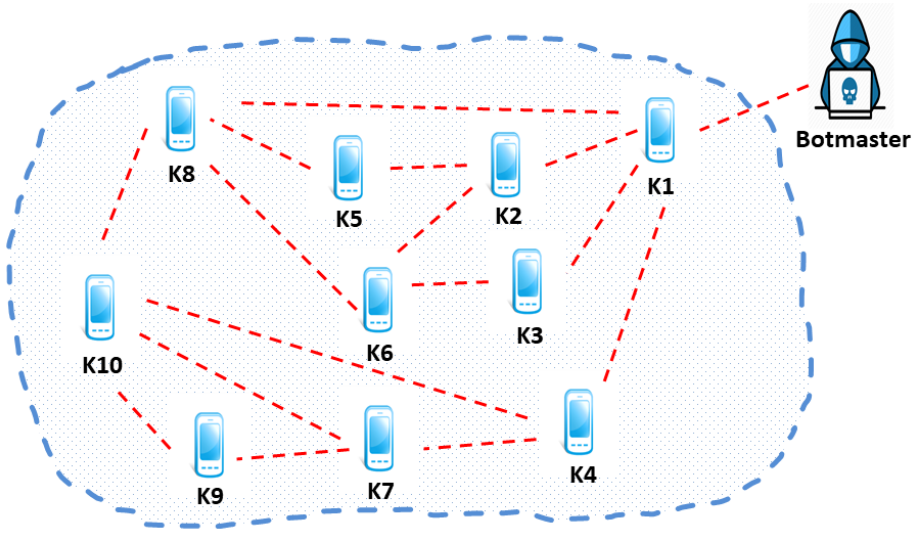


Figure 5.1: An epidemic SMS-based cellular botnet.

command (malware) as a SMS message to susceptible cdevices, no direct communication will prevail between the botmaster and those cdevices. Therefore, the malware propagation communication procedure is conducted as follows:

- The botmaster sends the malicious command as a SMS message to the seed cdevice.
- The seed cdevice starts acting as the C&C server in the cellular botnet, by propagating the malware to the susceptible cdevices in the network via its most central directly connected peers.
- After sending the malware to the seed's peers, each peer starts disseminating the malware to its most central peers, and the process continues until the propagation mechanism is completed.

Every cdevice in our proposed SMS-based cellular botnet performs the epidemic flooding algorithm as described in Algorithm 3, to regulate the malware propagation mechanism. As shown in the sample of our proposed epidemic SMS-based cellular botnet in Figure 5.1, the botmaster initiates the malware dissemination by dispatching the malware to the seed (i.e. the hub), which is $K1$ cdevice in this sample network. Then, the seed forwards the

malware to its most central neighbors (e.g. $K2$, $K3$, $K4$, and $K8$) in different random forwarding times to avoid the group-messaging mechanism. After that, each one of the cdevices $K2$, $K3$, $K4$, and $K8$ disseminates the malware to its most central neighbors in different random forwarding times, excluding the source sender of the malware, which is $K1$ in this case, to avoid the malware dissemination duplication, and consequently enhancing the efficiency of the propagation mechanism. For instance, cdevice $K4$ will transmit the malware to cdevices $K7$ and $K10$, and excludes its neighbor $K1$, because it is the source sender of the malware in this propagation cycle between $K1$ and $K4$. And the same method of malware propagation cycles is applied to the other neighbors in the cellular botnet network.

Our epidemic flooding algorithm in Algorithm 3 is implemented in every cdevice, to imitate the SMS-based C&C channel in our proposed cellular botnet. The epidemic flooding algorithm represents the core of the cellular botnet, which consists of four main aspects as follows:

1. The group-messaging mechanism, which refers to the process of propagating the malware to all peers at the same time, is not deployed in our flooding algorithm. Instead, in each propagation cycle, the sender disseminates the malware to its neighbors one by one at different random times. The time of sending the malware to each peer in a propagation cycle is measured in seconds, which is chosen randomly from the interval [60, 120].

2. There is no malware dissemination duplication. In each propagation cycle, the sender spreads the malware to its directly connected peers, excluding the source sender of the malware. In other words, the source cdevice which sent the malware to the current sender in a prorogation cycle will be eliminated.

3. The forwarding bound technique is implemented in the flooding algorithm, which refers to the total number of malicious SMSs (β) that can be sent by the source sender to its

directly connected peers in every propagation cycle. Every cdevice in our proposed cellular botnet can send no more than 4 malicious SMSs to its directly connected cdevices in each propagation cycle.

4. In every malware propagation cycle, the sender cdevice chooses the most central neighbors based on the cdevice degree centrality, to be the receivers of the malicious SMS in the current cycle.

By deploying the previous four main aspects of our flooding algorithm, we guarantee the epidemic behavior of our proposed SMS-based cellular botnet.

For our proposed model, the output of Algorithm 2 will be fed as input to Algorithm 3. In this context, the botmaster will be having full control on the C&C server (i.e. the seed), which holds the information about the network topology. In addition, it should be noted that in Algorithm 2 two matrices will be generated. The first matrix is an adjacency matrix that has size of 2000×2000, which represents the topology of the cellular botnet that shows the relationship between every pair of nodes in the network. And the second matrix has size of 2000×4, which shows information about each cellular device in the network, such as the device ID, device degree, and if a device represents a receiver or sender in the network. Later on, the two matrices will be used by Algorithm 3 to deploy the malware propagation mechanism.

Algorithm 2

Input:

$AMat$: represents the adjacency matrix.

$n\_cdevice$: represents the column size of the $AMat$.

Output:

$cdevice\_data$: represents a matrix of size n_cdevice $\times$ 4,

the 4 columns are: label, degree, get, and forward.

$degree\_i$: the degree of each cdevice i in the network,

$peers\_i$: the set of neighbors for every cdevice i in the network,

where $i = 1, ..., n\_cdevice$.

1: start;

2: **for** $\forall\ i \in n\_cdevice$ **do**

3: $degree\_i = \sum_{j=1}^{n\_cdevice} AMat(i, j)$

4: $peers\_i = \{AMat(i, j) \mid AMat(i, j) = 1, \forall\ j = 1,...,n\_cdevice\}$

5: cdevice_data(i, $label$) = i

6: cdevice_data(i, $degree$) = $degree\_i$

7: cdevice_data(i, get) = 0

8: cdevice_data(i, $forward$) = 0

9: **end for**

10: seed = hub(1,...,$n\_cdevice$)

11: **end**

Algorithm 3 Epidemic flooding algorithm deployed in the SMS-based cellular botnet

Input:

$cdevice\_data$: the matrix that contains the data of each cellular

phone device in the network.

$n\_cdevice$: the total number of cellular phone devices in the network.

t_spread: represents the propagation time in the network.

$peers\_i$: the set of neighbors for every cdevice in the network,

where $i = 1, ..., n\_cdevice$.

```
1:  start;
2:  cdevice_data(seed, get) = 1;
3:  flag = 1;
4:  while flag = 1 do
5:      for ∀ cdevice i ∈ n_cdevice do
6:          count = 0
7:          peer = peers_i
8:          cdevice_data_i = cdevice_data(i,:), i ∈ peer ∧ cdevice_data(i, get) = 0 ∧
            cdevice_data(i, forward) = 0
9:          Sort cdevice_data_i, using the column degree in a descending order.
10:         Set n_forward as row size in cdevice_data_i.
11:         if n_forward = 0 then
12:             cdevice_data(i,forward) = 1
13:         else
14:             t_forward = cdevice_data(i,get)
15:             for ∀ s ∈ (1, min(4, n_forward)) do
16:                 t_forward = t_forward + Random[60sec, 120sec]
```

```
17:                 if t_forward ≤ t_spread + 1 then
18:                     cdevice_data( cdevice_data_i (s, label), get) = t_forward
19:                     count = count + 1
20:                 end if
21:             end for
22:             cdevice_data(i,forward) = 1
23:         end if
24:     end for
25:     if count = 0 then
26:         flag = 0
27:     end if
28: end while
29: total number of infected cdevices = ∑_{i=1}^{n_cdevice} 1_{(cdevice_data(i,get)>0)}
30: end
```

5.2.2 Topology Analysis

Our proposed epidemic SMS-based cellular botnet represents an undirected graph: $G = (V, E)$, where V indicates the set of vertices (i.e. cellular phone devices), and $V = \{v_1, v_2, ..., v_n\}$, where $n = |V|$.

E indicates the set of edges (i.e. links) between cellular phone devices in the cellular botnet. Each element of E is an edge, $e = (i, j)$, which indicates an unordered pair. We say i and j are connected and write $i \sim j$ if $(i, j) \in E$.

Our proposed SMS-based cellular botnet network is represented as an adjacency matrix, which is denoted as $AMat = (AMat_{ij})$, where $i, j \in V$. $AMat$ matrix is $n \times n$ symmetric binary matrix, with all the diagonal elements equal to 0 (i.e. no self-edges in our cellular botnet network).

$$AMat_{ij} = 1_{\{i \sim j\}} = \begin{cases} 1, & \text{if } (i, j) \in E \\ 0, & \text{otherwise} \end{cases} \tag{5.1}$$

The linked peers of a given vertex $v \in V$ is defined as $(v) = u \in V : u \sim v$ (i.e. the set of neighbors that are directly connected to vertex v). Then the set of peers for every cellular device (i) can be written in terms of the adjacency matrix as:

$$peers\_i = \{AMat(i, j) \mid AMat(i, j) = 1, \ \forall\, i \text{ and } j = 1, ..., n\} \tag{5.2}$$

The degree of vertex v is defined as $k_v = \lceil N(v) \rceil$ (i.e. the number of neighbors of vertex v). Then the degree of each cellular device (i) can be described in terms of the adjacency matrix as:

$$k_i = degree\_i = \sum_{j=1}^{n} AMat(i, j) \tag{5.3}$$

Every edge in the undirected network has two ends, and if the total number of edges is m, then there are $2m$ ends of edges in the network. Therefore, the number of ends of edges

equals the sum of the degrees of all the cellular devices in the network.

$$2m = \sum_{i=1}^{n} k_i = \sum_{ij} AMat(i,j) \tag{5.4}$$

Then the mean degree c of a cellular device

$$c = \frac{1}{n} \sum_{i=1}^{n} k_i \tag{5.5}$$

the mean degree c can be written as:

$$c = \frac{2m}{n} \tag{5.6}$$

Therefore, the effectiveness of the epidemic behavior of our proposed SMS-based cellular botnet is highly determined by the topology of the cellular botnet graph.
As a result, we have chosen three different random graph models as candidate topologies for our proposed botnet, and the goal is to determine which of these topologies yields the most efficient epidemic behavior.

A random graph is a graph model where certain properties are fixed, and all the other properties of the graph are kept random, which is defined on a probability space (Ω, F, P), and with a probability distribution.

The evolution of our cellular botnet network model starts with isolated cellular phone devices with no connections between them at the initial stage of the network model establishment. Then for our botnet model to be established, two or more cellular phone devices start connecting to each other; the connection between two cellular phone devices happens by using a link. Then, another two or more cellular phone devices start connecting to each other until the whole cellular botnet network is created. In other words, the process of generating the cellular botnet network could be thought of as a ”matching process” or ”pairing process” between different cellular phone devices in the network.

In our undirected graph $G = (V, E)$, the degree of a cellular device is (k), and the fraction of cellular phone devices that have degree k is (P_k), where P_k is the degree distribution that indicates the frequency that cellular phone devices with different degrees appear in the cellular botnet network. In other words, the degree distribution P_k represents the probability that a randomly chosen cellular phone device in the cellular botnet network has degree k.

Degree distribution is the most fundamental property of random graphs, that has a huge impact on the networks, and provides a better way to understand the behavior of networks. Therefore, the analysis of our proposed cellular botnet network relies on the study of the degree distribution of the random graph models.

$$P_k = P(k_v = \lceil N(v) \rceil) \tag{5.7}$$

Where P_k is the degree distribution, and k_v is the degree of vertex v, which is also represented by $\lceil N(v) \rceil$.

In this Chapter, we study 3 random graph models as candidate topologies for our proposed cellular botnet network, namely, Barabasi–and-Albert topology (BAT), Erdos-and-Reyni topology (ERT), and Watts-and-Strogatz topology (WST).

5.2.2.1 Barabasi–and-Albert Topology

The BAT is a preferential attachment model (PAM), which is developed by applying a multi-phases mechanism, where in each phase, new vertices (cdevices) and edges (links) join the cellular network. At the end of the process, the obtained BAT graph represents the network model that has a majority of vertices with low degrees and a minority of vertices with high degrees (i.e. power-law degree distribution). The BAT model has a degree distribution that follows the power-law distribution (Pareto distribution), hence, it represents a scale-free network. The power-law degree distribution is a right-skewed degree distribution, meaning a network degree distribution that has a long right tail shape of high-degree

nodes. Consequently, the attachment probability distribution on the set of vertices (i.e. cdevices), where $V = \{v_i : i = 1, ..., n\}$ is:

$$\pi(v_i) = \frac{k_{v_i}}{\sum_j k_{v_i}} \tag{5.8}$$

where k_{v_i} is the degree of cdevice v_i, and $\sum_j k_{v_i}$ is the sum of degrees of all cdevices in the network.

And the degree distribution of the BAT model that follows the power-law distribution is given by:

$$P_k = P(k_v = \lceil N(v) \rceil) \approx Sk^{-\alpha} \approx 2m^{1/\beta}k^{-\alpha} \tag{5.9}$$

where $\beta = 1/2$, and α which is the exponent of the power law $= 3$.

5.2.2.2 Erdos-and-Reyni Topology

The Erdos-and-Reyni Topology (ERT) is a model that has n nodes, and the edge between each distinct pair of nodes is placed with an independent probability (p), which means that the probability of placing an edge between a pair of nodes is independent from placing every other edge between other pair of nodes in the network. At the beginning of establishing the network, all the n nodes are assumed to be unconnected, and the construction of the network starts with placing an edge between two random nodes. Then, this is repeated several times until the complete network is built. Following this procedure, we randomly place the edges between the pairs of nodes with probability p. Therefore the average number of edges in the network is obtained as:

$$m = \binom{n}{2} p \tag{5.10}$$

where $\binom{n}{2}$ is the number of pairs of nodes, and p is the number of edges between a pair of nodes.

The ERT model has a degree distribution that follows the binomial distribution, thus, its degree distribution is determined by:

$$P_k = P(k_v = \lceil N(v) \rceil = k) = \binom{n-1}{k} p^k (1-p)^{n-1-k} \tag{5.11}$$

Where P_k is the degree distribution, $k_v = k$ is the degree of vertex v, n represents the total number of nodes in the network, and p is the number of edges between a pair of nodes.
And the average of degree (k) in the ERT model is given by:

$$k = c = \left\langle \frac{2m}{n} \right\rangle = \frac{2\langle m \rangle}{n} = \frac{2}{n}\binom{n}{2} p = (n-1)p \tag{5.12}$$

Where m is the number of edges in the network, n represents the number of nodes in the network, and p is the number of edges between a pair of nodes.
The ERT model is also known as a Poisson random graph. Therefore, when $n \to \infty$, the binomial degree distribution becomes the Poisson degree distribution, given by:

$$P_k = P(k_v = \lceil N(v) \rceil) = e^{-z} \frac{z^k}{k!} \tag{5.13}$$

where $z = c = \dfrac{2m}{n}$ is the value of the average degree.

5.2.2.3 Watts-and-Strogatz Topology

The construction of the WST model starts with a regular lattice of n nodes arranged as a circle, where every node is attached by edges to its average node degree (c) peers. Then, the edges in the circle network are randomly rewired following an independent probability (p). Here, the rewiring mechanism means moving the edges from their current positions to new random positions in the circle. By the definition of the WST model, having a value $p > 0$ of the rewiring probability, the establishment of the WST network will be formed in a way similar to that of a random graph. Therefore, we have chosen $p = 0.5$.

5.3 Performance Evaluation

Our proposed epidemic SMS-based cellular botnet is evaluated using the BAT, ERT, and WST as topologies for the cellular botnet network, respectively. The goal is to determine which of these topologies yields the most efficient epidemic behavior in terms of stealth and speed characteristics for the C&C channel. For implementation purpose, we have used the R packages of the igraph network analysis software. In each simulation, 20 graphs for each topology have been deployed, and the performance of our proposed epidemic SMS-based cellular botnet in terms of forwarding bound, average cdevice degree, cellular botnet size, and cdevice failure paradigm, have been investigated.

5.3.1 The igraph Simulator

igraph is a network analysis tool that is used for creating and manipulating graphs and analyzing networks, it is available as Python and R packages. The software is widely used in academic research, in the field of complex networks such as telecommunication networks, computer networks, and its related fields. igraph is open source and capable of handling large networks efficiently [59] [60].

5.3.2 Simulation Results

5.3.2.1 Effects of the forwarding bound

Forwarding bound represents the maximum number of malicious SMSs a sender cdevice can disseminate to its directly attached peers in every propagation cycle, where each peer can receive only one malicious SMS. The value of the forwarding bound should be less than the value of the cdevice degree. In our epidemic flooding algorithm, we set the value of the forwarding bound to four, but for investigation purposes, and to study the impact of this feature on the performance of our proposed cellular botnet, we will study another two

values of forwarding bound: three and two.

The main goal of deploying this feature is to enhance the epidemic behavior of our proposed cellular botnet by reducing the probability of detecting cellular botnet traffic. In this scenario, the number of cdevices in the network is set to 2000, and the average cdevice degree is set to 6.

We found that the ERT model represents the optimal topology for our cellular botnet network compared to the other two models, WST and BAT, when every cdevice dissimulates no less than 4 malicious messages to its directly connected peers in every propagation cycle, as shown in Figure 5.2.

Figure 5.2 depicts the 20 runs for the 20 graph samples of each topology of the three graph models, and their corresponding number of infected cdevices, within 9 minutes of malware propagation time. Furthermore, the average number of infected cdevices with the malicious SMS in the ERT model is 1921, which is followed by the WST model that has 1702 infected cdevices, and the BAT model that has 1550. The poor performance of the BAT model can be attributed to the behavior of its cdevice degree distribution, which is a power-law distribution with a long right tail shape.

Both Figures 5.3 and 5.4 illustrate the scenario where each cdevice in the network can forward only 3 and 2 malicious messages, respectively. Both of these two cases show that the ERT model is the optimal topology (over WST and BAT), which has an average number of infected cdevices of 1698 when the forwarding bound = 3 and 916 when the forwarding bound = 2. Also, it is found that the WST model has an average number of infected cdevices of 1528 when the forwarding bound = 3 and 860 when the forwarding bound = 2. Besides, the BAT is the worst topology with an average number of infected cdevices of 1305 when the forwarding bound = 3 and 530 when the forwarding bound = 2. The insights that are learned from deploying this feature in the proposed epidemic cellular botnet are: increasing the value of forwarding bound will definitely increase the number of infected mobile devices in the deployment of all the three toplogies (ERT, BAT, WST).

Also, the ERT model will be always the optimal topology for enhancing the epidemic behavior of cellular botnets regardless of the deployed value of the forwarding bound. Moreover, the BAT model will be always the best topology for mitigating/reducing the epidemic behavior of cellular botnets regardless of the deployed value of the forwarding bound. In addition, setting the forwarding bound value to 4 will satisfy the best epidemic efficiency rate in the cellular botnets.

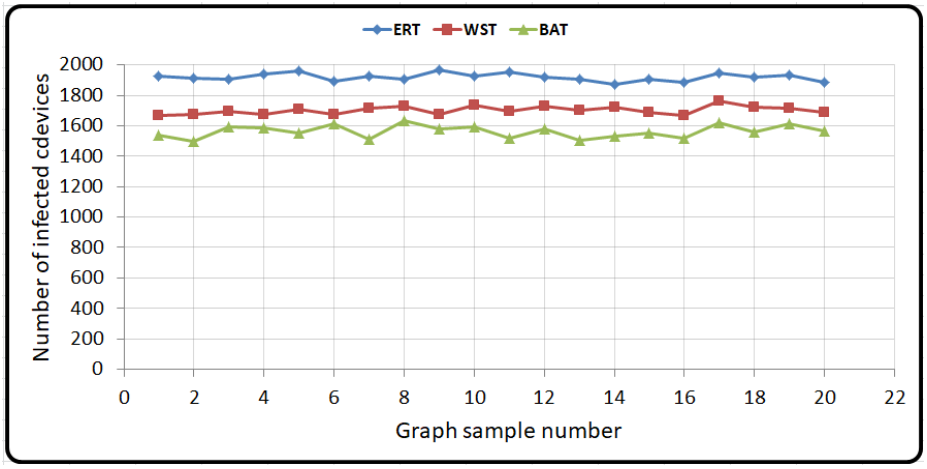


Figure 5.2: Forwarding Bound = 4

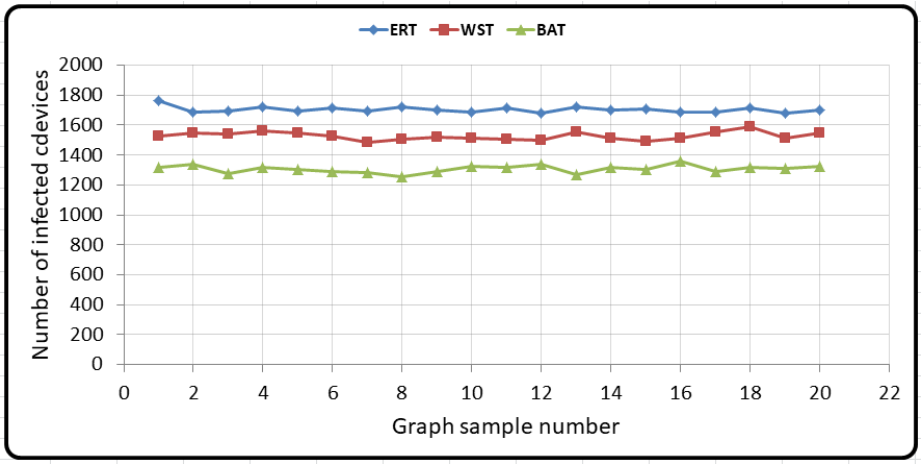


Figure 5.3: Forwarding Bound = 3

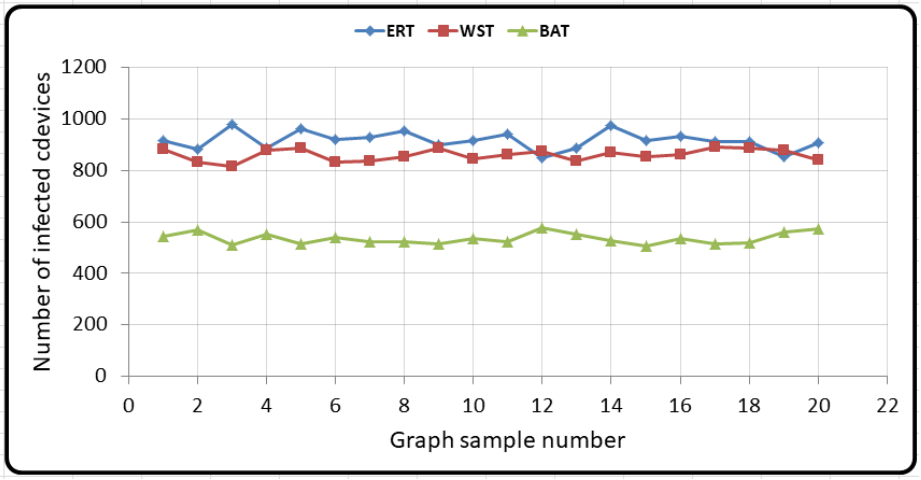


Figure 5.4: Forwarding Bound = 2

5.3.2.2 Effects of the average cdevice degree

The cdevice degree indicates the number of directly connected peers for each cdevice in the network. The Average Cdevice Degree (ACD) is set to 6 in our proposed SMS-based cellular botnet, but to study the impact of this feature on the epidemic behavior of our proposed cellular botnet, we have tested two more values of ACD, which are 4 and 8. In this scenario, the cellular botnet size is set to 2000, and 4 is set as the forwarding bound value. The results of the simulation show that the higher the value of ACD, the better the performance of our proposed cellular botnet in terms of the number of infected cdevices in the network for all the three topology models (ERT, WST, and BAT). In other words, increasing the number of the directly attached neighbors for each cdevice in the network leads to boosting the number of malicious SMS forwarding events in every propagation cycle, and consequently, enhancing the epidemic behavior of our proposed cellular botnet by raising the number of the infected cdevices.

The impact of the three values of ACD for the ERT model, after 9 minutes of malware propagation time is depicted in Figure 5.5. Figure 5.5 shows the 20 runs for the 20 ERT graph samples for each value of ACD, in terms of the number of infected cdevices in the network. As a result, when the ACD value is 8, almost all the cdevices in the network of

the ERT model are infected with the malicious SMS. This number drops to 96% when the ACD value is 6 and 65% when the ACD value is 4.

Figure 5.6 illustrates the 20 runs for the 20 WST graph samples for each value of the three different values of ACD. It is observed that the rate of infected cdevices is 90% when the ACD value is 8, 85% when the ACD value is 6, and 55% when the ACD value is 4. For the BAT model, the results are captured in Figure 5.7, where it is observed that the rate of infected cdevices is 85% when the ACD value is 8, 77% when the value of ACD is 6, and 48% when the ACD value is 4.

The insights that are learned from deploying this feature in the proposed epidemic cellular botnet are: increasing the value of average cellular device degree will definitely increase the number of infected mobile devices in the deployment of all the three toplogies (ERT, BAT, WST). Also, the ERT model will be always the optimal topology for enhancing the epidemic behavior of cellular botnets regardless of the deployed value of the average cellular device degree. Moreover, the BAT model will be always the best topology for mitigating/reducing the epidemic behavior of cellular botnets regardless of the deployed value of the average cellular device degree. In addition, setting the average cellular device degree value to 6 will satisfy the best epidemic efficiency rate in the cellular botnets.

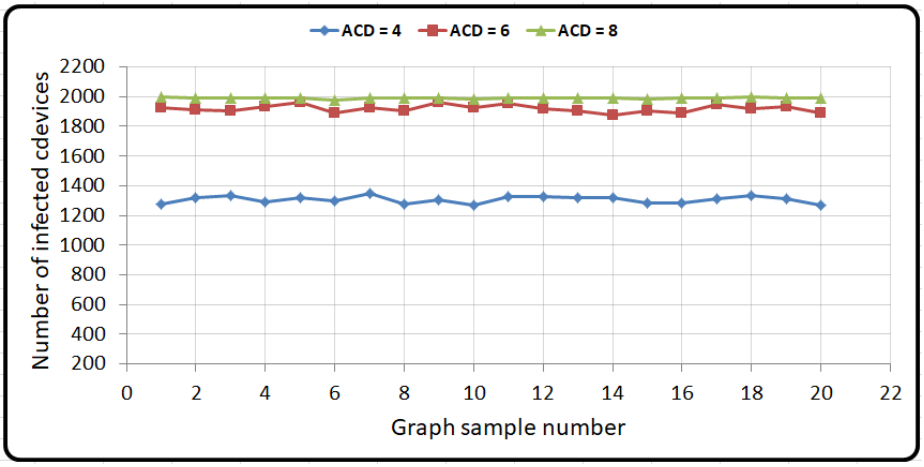


Figure 5.5: ACD of ERT

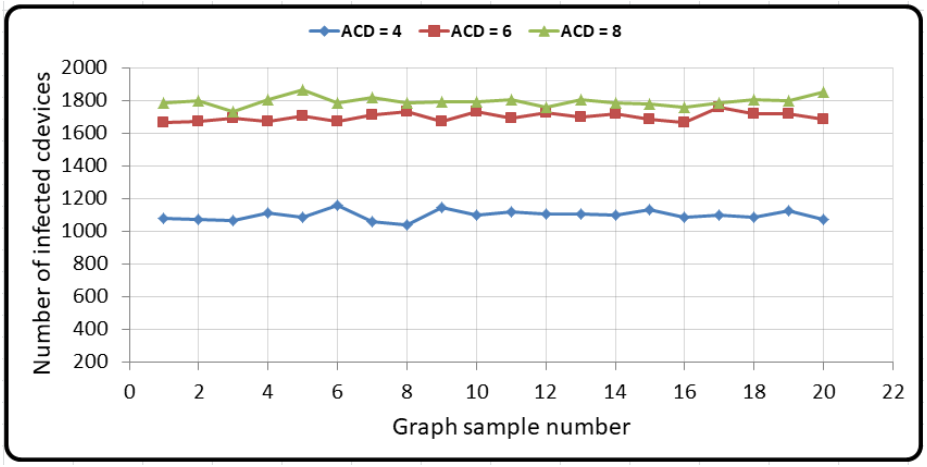


Figure 5.6: ACD of WST

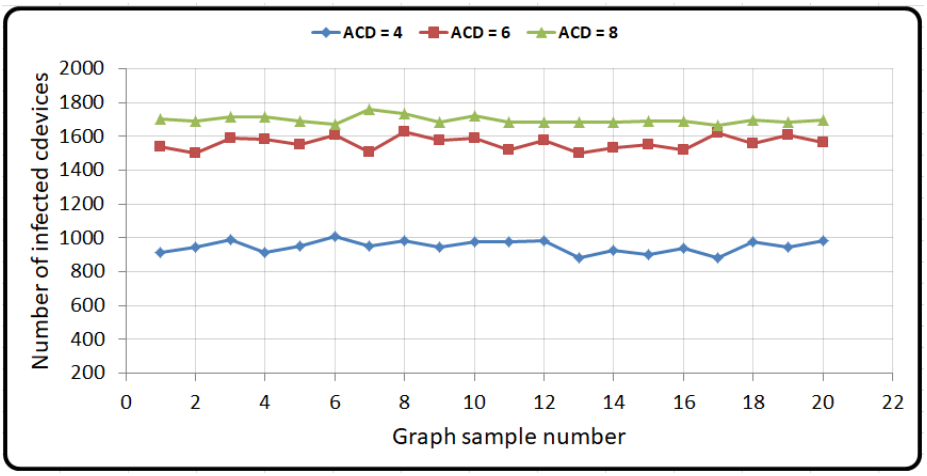


Figure 5.7: ACD of BAT

5.3.2.3 Effects of the cellular botnet size

In this scenario, we have investigated the influence of three different cellular botnet sizes on the epidemic behavior of our cellular botnet: cellular botnet size of 1500 cdevices, 1000 cdevices, and 500 cdevices. In this scenario, the average cdevice degree is 6, and the forwarding bound is set to 4. The results of the simulation show that the ERT model is the best topology for the three different cellular botnet sizes.

Figure 5.8 depicts the results for the ERT model, showing an average number of infected cdevices of 990 when the botnet size is 1500, 860 when the botnet size is 1000, and 480 when the botnet size is 500, respectively. For the WST model, the results for the same are captured in Figure 5.9, which reveal an average number of infected cdevices of 900 (for a botnet size of 1500), 700 (for a botnet size of 1000), and 425 (for a botnet size of 500), respectively. Finally, for the BAT model, the average number of infected cdevices is 825 (for a botnet size of 1500), 650 (for a botnet size of 1000), and 400 (for a botnet size of 500), respectively.

The insights that are learned from deploying this feature in the proposed epidemic cellular botnet are: increasing the size of cellular botnets will increase the number of infected mobile devices in the deployment of all the three toplogies (ERT, BAT, WST). Also, the ERT model will be always the optimal topology for enhancing the epidemic behavior of cellular botnets regardless of the cellular botnet size. Moreover, the BAT model will be always the best topology for mitigating/reducing the epidemic behavior of cellular botnets regardless of the cellular botnet size.

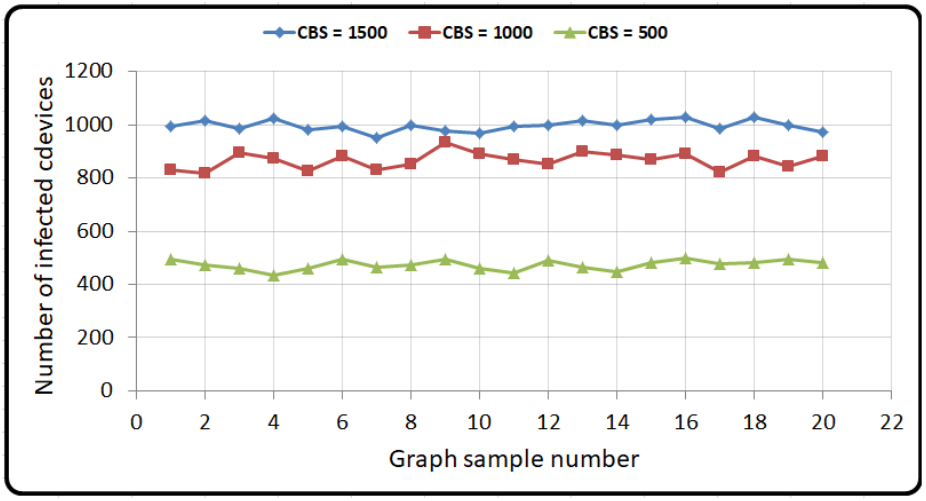


Figure 5.8: CBS of ERT

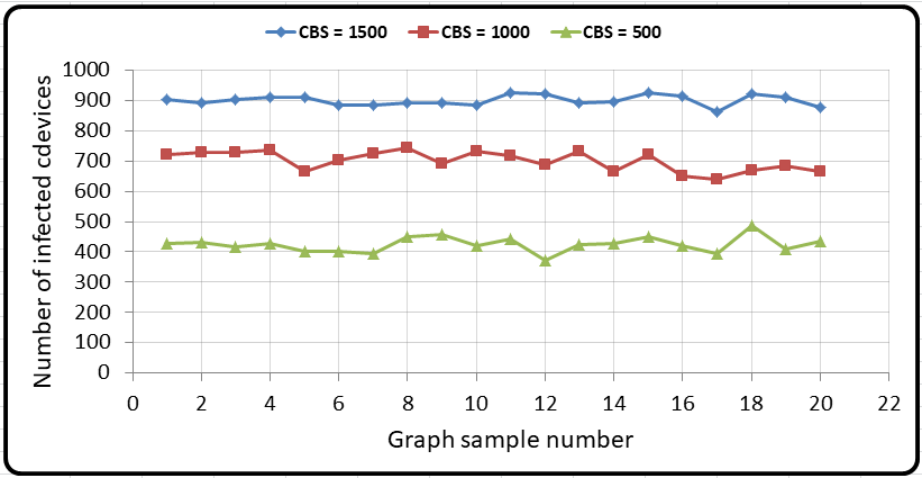


Figure 5.9: CBS of WST

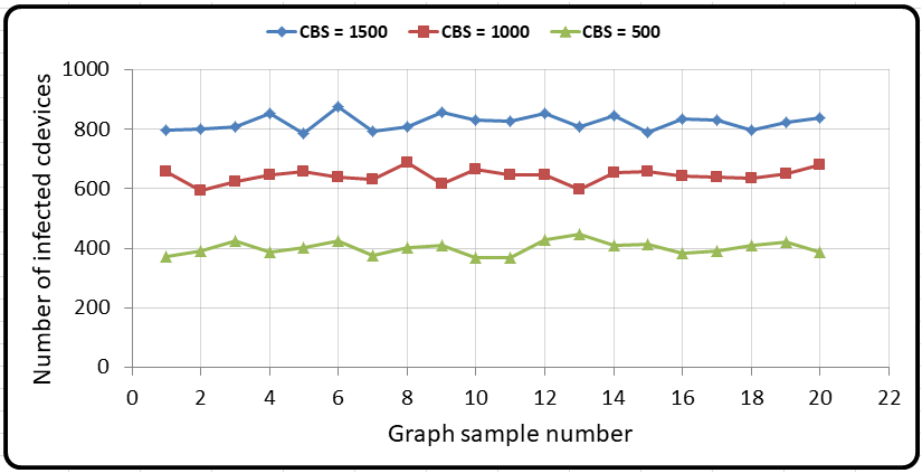


Figure 5.10: CBS of BAT

5.3.2.4 Effects of the cdevice failure paradigm

Cellular phone devices are some of the main components of the cellular networks, and these devices could face technical problems (e.g. hardware, software, or battery problems) that lead to losing the communication capabilities (e.g. sending data to other cellular devices or receiving data from other cellular devices), halting or shutdown, and therefore the cellular devices may not be able to receive any type of data, such as a malicious SMS. This scenario is known as the cdevices failure paradigm.

We now study the case of cdevices failure in our proposed botnet. The goal is to measure

the resistance of the botnet against such failure. To this end, we have considered the ERT, WST, and BAT topology models under two cdevice failure paradigms: random and selective.

In the random cdevice failure paradigm, 10% of the cdevices from the cellular botnet which corresponds to a size of 2000 are randomly eliminated, the average cdevice degree is set to six, and the forwarding bound is set to four. Then, we investigate the impact of this elimination on our proposed cellular botnet, by deploying the three topology models. Figure 5.11 depicts the scenario of running the simulation of the random cdevice failure after 9 minutes of propagation time. As a result, the ERT model represents the most resistant topology in opposition to the random cdevice failure, which has an average number of infected cdevices of 1220. Followed by the WST model, which has an average number of infected cdevices of 1110, and the least resistant topology is the BAT model which has 840 cdevices as the average number of infected cdevices.

In the selective cdevice failure paradigm, 10% of the most central cdevices (i.e. cdevices with the highest degrees) are eliminated from the cellular botnet which corresponds to a size of 2000, the average cdevice degree is set to six, and the forwarding bound is four. Figure 5.12 shows the results of running the simulation of the selective cdevice failure paradigm. The ERT model remains the most resistant topology in this scenario, with an average number of 680 infected cdevices, and a resistance reduction of 44% compared to the random cdevice failure paradigm. Furthermore, the WST model has an average number of 570 infected cdevices, and the BAT model remains the least resistant topology with an average number of 453 infected cdevices. Thus, according to the results in Figures 5.11 and 5.12 of the two scenarios, the ERT model is the most robust topology compared to the random cdevice failure paradigm and the selective cdevice failure paradigm.

The insights that are learned from deploying this feature in the proposed epidemic cellular botnet are: The ERT model will be always the optimal topology for enhancing the epidemic behavior of cellular botnets in the case of deploying the random cellular device failure ap-

proach and the selective cellular device failure approach. Moreover, the BAT model will be always the best topology for mitigating/reducing the epidemic behavior of cellular botnets in the case of deploying the random cellular device failure approach and the selective cellular device failure approach.

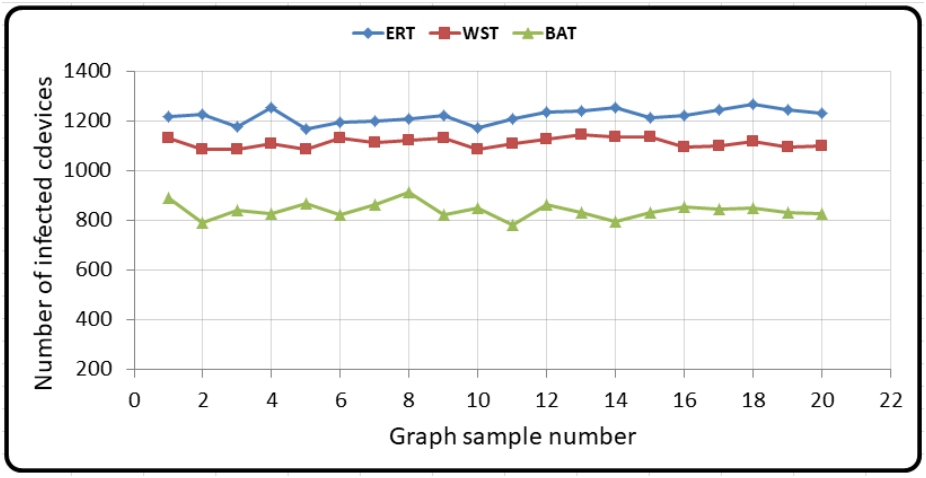


Figure 5.11: Random cdevice failure

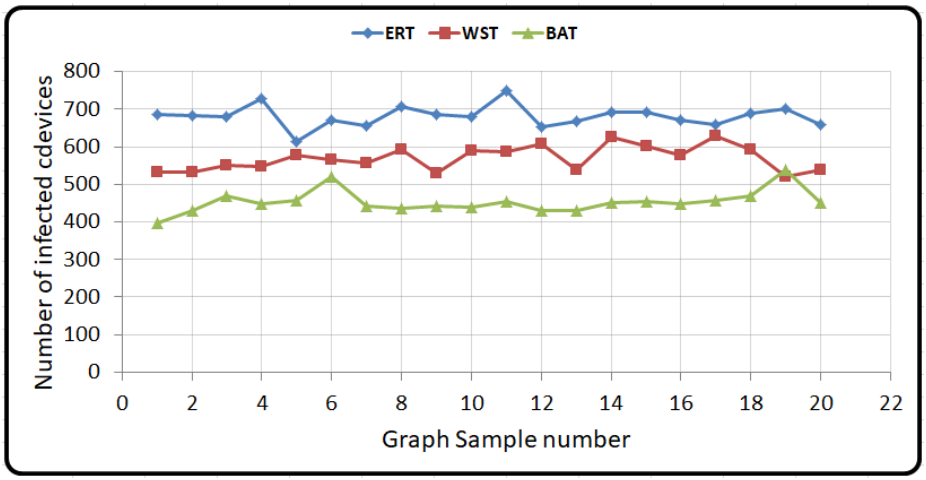


Figure 5.12: Selective cdevice failure

5.3.3 Comparative Analysis

The performance characteristics of the epidemic behavior of our SMS-based cellular botnet model are compared to the Hua-Sakurai model in [32].

Our proposed model relies on the hub node approach as a mechanism for selecting the seed (C&C server) in a cellular botnet, and on the most-central node approach as a mechanism for selecting the neighbors of each node in the cellular botnet as the receivers of the malware commands in every propagation cycle. While in [32], the authors in their cellular botnet design relies on the random node approach as a mechanism for choosing the seed, and also deploy the random node approach as a mechanism for choosing the receivers of the malware commands.

Moreover, the results of our study show that our proposed cellular botnet model has higher epidemic behavior, and outperforms the model in [32].

By applying 2000 cdevices as the cellular botnet size, each cdevice has 6 neighbors on average, and every cdevice can disseminate no more than 4 malicious SMS messages. Then, a malicious SMS can be propagated to 96% of the vulnerable cdevices in the network within 9 minutes, compared to 90% of the propagation population within 14 minutes in [32].

Furthermore, the study shows that our proposed epidemic SMS-based cellular botnet is more robust against the random cdevice failure paradigm and the selective cdevice failure paradigm. Table 5.1 shows a comparison between our SMS-based cellular botnet model and the model in [32].

Table 5.1: Hua-Sakurai model vs. Our model

Parameter	**Hua-Sakurai Model**	**Our Model**
Number of nodes	2000	2000
Number of peers	6 neighbors	6 neighbors
Propagation population	90%	96%
Propagation time	14 minutes	9 minutes
Number of SMS messages	4	4
SMS receivers per propagation cycle	Random node selection	Central node selection
Random node failure	robust	robust
Selective node failure	robust	robust
Flooding algorithm	naive	advanced
Seed selection	Random selection	Hub selection
Number of random graphs	3 models	3 models

5.4 Summary

In this chapter, we have proposed an epidemic SMS-based cellular botnet whose operation relies on a developed epidemic flooding algorithm that initiates a Smishing attack (i.e. SMS phishing attack). We have evaluated it using the BAT, ERT, and WST as topologies for the cellular botnet network, respectively, to determine which of these topologies yields the most efficient epidemic behavior in terms of stealth and speed characteristics of the C&C channel, and consequently, finding a mitigation mechanism for such behavior. Simulation results have shown that ERT is the optimal topology for enhancing the epidemic behavior of a cellular botnet, and the BAT model is the best topology for mitigating an epidemic behavior. We showed that our proposed epidemic SMS-based cellular botnet is resistant and resilient to random and selective cdevice failures in the case of the ERT model, and less resistant in the case of the BAT model.

The contribution in this chapter can be described in our ability to develop and deploy an epidemic flooding algorithm as C&C mechanism that satisfies an optimal efficiency rate

(96% in 9 minutes) for the epidemic behavior of cellular botnets. Also, our ability to clearly stating and defining the characteristics of epidemic cellular botnets by deploying an epidemic C&C mechanism that employs 4 main aspects, namely, no group-messaging mechanism, no malware dissemination duplication, deployment of the forwarding bound technique, and implementation of the most-central node approach.

Chapter 6

Conclusion

6.1 Summary

In this research, a mobile botnet that conducts a DDoS attack over a LTE network has been proposed. Our simulation results reveal that using the SMM model is advantageous compared to the AMM model in terms of (1) number of infected mobile devices, (2) CPU resource consumption, (3) task processing time consumed, (4) Web server HTTP traffic load over time, (5) receiving HTML objects, all in the victim Web server; and (6) the number of bits successfully transmitted to the victim Web server. This suggests that using the AMM model would yield a more severe threat impact of the mobile botnet on the victim Web server compared to using the SMM model. In other words, having higher level of asymmetric mobility (i.e. random movements patterns) of mobile devices in LTE network leads to a higher number of infected mobile devices, and consequently leads to a higher threat impact.

In addition, this research has proposed a mobile botnet model that launches a DDoS attack against a victim web server. The impact of two base transceiver station selection mechanisms, namely, DBM and SPBM on the proposed mobile botnet is investigated by simulations, showing that the DBM mechanism yields a higher threat impact on the victim server compared to the SPBM mechanism, in terms of (1) total number of infected mobile

devices, (2) consumed CPU resource, (3) total amount of uplink MAC traffic sent by all mobile devices, (4) Uplink throughput of all eNodeB stations, and (5) HTTP traffic load consumed by the victim server over time. As a result, having eNodeB stations in the LTE network that are selected based on the distance factor only (i.e. the shortest distance) yields to a higher threat impact on the victim server compared to the mechanism of selecting eNodeB stations based on the signal power factor (i.e. the highest value of RSRP).

Furthermore, in this research, we have proposed an epidemic SMS-based cellular botnet whose operation relies on a developed epidemic command and control mechanism, which initiates a Smishing attack (i.e. SMS phishing attack). We have evaluated it using the BAT, ERT, and WST as topologies for the cellular botnet network, respectively, to determine which of these topologies yields the most efficient epidemic behavior in terms of stealth and speed characteristics of the C&C channel, and consequently, finding a mitigation mechanism for such behavior. Simulation results have shown that ERT is the optimal topology for enhancing the epidemic behavior of a cellular botnet, and the BAT model is the best topology for mitigating an epidemic behavior. We showed that our proposed epidemic SMS-based cellular botnet is resistant and resilient to random and selective cdevice failures in the case of the ERT model, and less resistant in the case of the BAT model. The results showed that the higher the value of forwarding bound (i.e. the maximum number of messages a sender node can disseminate to its attached peers), the higher the number of infected mobile devices. In addition, increasing the average number of directly connected peers for each cellular device in the network, leads to a higher number of infected mobile devices. Furthermore, having a higher size of a mobile botnet yields to a higher number of infected mobile devices.

6.2 Future Work

In future work, we plan to investigate other LTE-based mobility models and study their impact on the behavior of mobile botnets. We also plan to investigate the malware propagation impact when more eNodeB stations and EPC nodes are added to the considered LTE network topology. The botnet model proposed in this work can inspire the design of effective and efficient techniques for detecting and preventing the impact of mobile botnets. Our future work also includes the intensive study of cellular network components, features, operations, and their impact on the epidemic behavior of cellular botnets. In the future, we also intend to use the results of this research to design, test, and evaluate a baseline and foundation for effective and efficient techniques for detecting cellular botnets and revealing their behaviors over cellular networks such as 4G networks and 5G networks.

Bibliography

[1] Khyati Vachhani. Security threats against lte networks: A survey. In *International Symposium on Security in Computing and Communication*, pages 242–256. Springer, 2018.

[2] Andrea Goldsmith. *Wireless communications*. Cambridge university press, 2012.

[3] Verne H Mac Donald. Advanced mobile phone service: The cellular concept. *The bell system technical Journal*, 58(1):15–41, 1979.

[4] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, and Mika Ylianttila. Security for 5g and beyond. *IEEE Communications Surveys & Tutorials*, 21(4):3682–3722, 2019.

[5] Timo Halonen, Javier Romero, and Juan Melero. *GSM, GPRS and EDGE performance: evolution towards 3G/UMTS*. John Wiley & Sons, 2004.

[6] Jochen H Schiller. *Mobile communications*. Pearson education, 2003.

[7] Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen, Siamäk Naghian, and Valtteri Niemi. *UMTS networks: architecture, mobility and services*. John Wiley & Sons, 2005.

[8] Harri Holma and Antti Toskala. *HSDPA/HSUPA for UMTS: high speed radio access for mobile communications*. John Wiley & Sons, 2007.

[9] David Astély, Erik Dahlman, Anders Furuskär, Ylva Jading, Magnus Lindström, and Stefan Parkvall. Lte: the evolution of mobile broadband. *IEEE Communications magazine*, 47(4):44–51, 2009.

[10] Stefania Sesia, Issam Toufik, and Matthew Baker. *LTE-the UMTS long term evolution: from theory to practice*. John Wiley & Sons, 2011.

[11] Ericsson mobility report. ericsson company, technology emerging business, november 2020. https://www.ericsson.com/4adc87/assets/local/mobility-report/documents/2020/november-2020-ericsson-mobility-report.pdf.

[12] Rath Vannithamby and Anthony C. K. Soong. *5G verticals: customising applications, technologies and deployment techniques*. John Wiley and Sons, Inc, 2020.

[13] Devaki Chandramouli, Rainer Liebhart, and Juho Pirskanen. *5G for the connected world*. John Wiley and Sons, Inc, 2019.

[14] Marios Anagnostopoulos, Georgios Kambourakis, and Stefanos Gritzalis. New facets of mobile botnet: architecture and evaluation. *International Journal of Information Security*, 15(5):455–473, 2016.

[15] José Martins, Catarina Costa, Tiago Oliveira, Ramiro Gonçalves, and Frederico Branco. How smartphone advertising influences consumers' purchase intention. *Journal of Business Research*, 94:378–387, 2019.

[16] David Dagon, Cliff Changchun Zou, and Wenke Lee. Modeling botnet propagation using time zones. In *NDSS*, volume 6, pages 2–13, 2006.

[17] Phillip Porras, Hassen Saidi, and Vinod Yegneswaran. An analysis of the ikee. b iphone botnet. In *International Conference on Security and Privacy in Mobile Information and Communication Systems*, pages 141–152. Springer, 2010.

[18] Xuetao Wei, Lorenzo Gomez, Iulian Neamtiu, and Michalis Faloutsos. Malicious android applications in the enterprise: What do they do and how do we fix it? In *2012 IEEE 28th International Conference on Data Engineering Workshops*, pages 251–254. IEEE, 2012.

[19] Najla Etaher, George RS Weir, and Mamoun Alazab. From zeus to zitmo: Trends in banking malware. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 1386–1391. IEEE, 2015.

[20] Shui Yu. *Distributed denial of service attack and defense*. Springer, 2014.

[21] Felix Lau, Stuart H Rubin, Michael H Smith, and Ljiljana Trajkovic. Distributed denial of service attacks. In *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems,*

humans, organizations, and their complex interactions'(cat. no. 0, volume 3, pages 2275–2280. IEEE, 2000.

[22] Cik Feresa Mohd Foozy, Rabiah Ahmad, and Mohd Faizal Abdollah. Phishing detection taxonomy for mobile device. *International Journal of Computer Science Issues*, 10(1):338–344, 2013.

[23] M Nazreen Banu and S Munawara Banu. A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies*, 4(6):783–786, 2013.

[24] Geumhwan Cho, Junsung Cho, Youngbae Song, and Hyoungshick Kim. An empirical study of click fraud in mobile advertising networks. In *2015 10th International Conference on Availability, Reliability and Security*, pages 382–388. IEEE, 2015.

[25] Tommy Blizard and Nikola Livic. Click-fraud monetizing malware: A survey and case study. In *2012 7th International Conference on Malicious and Unwanted Software*, pages 67–72. IEEE, 2012.

[26] Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor, and Wenke Lee. Evaluating bluetooth as a medium for botnet command and control. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 61–80. Springer, 2010.

[27] Datasets and tools by keyword: Dtn. http://crawdad.org/nus/bluetooth/20070903/.

[28] New york city subway dataset. https://jameskao.me/analyzing-the-nyc-subway-dataset/.

[29] KGS Yuanyuan Zeng, Xin Hu, and Kang G Shin. How to construct a mobile botnet? In *The 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2010)*, 2010.

[30] Feng Li, Yinying Yang, and Jie Wu. Cpmc: An efficient proximity malware coping scheme in smartphone-based mobile networks. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9, March 2010.

[31] Guining Geng, Guoai Xu, Miao Zhang, Yanhui Guo, Guang Yang, and Cui Wei. The design of sms based heterogeneous mobile botnet. *Journal of Computers*, 7(1):235–243, 2012.

[32] Jingyu Hua and Kouichi Sakurai. Botnet command and control based on short message service and human mobility. *Computer Networks*, 57(2):579–597, 2013.

[33] Zhuo Lu, Wenye Wang, and C. Wang. How can botnets cause storms? understanding the evolution and impact of mobile botnets. In *INFOCOM, 2014 Proceedings IEEE*, pages 1501–1509, April 2014.

[34] Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta. On cellular botnets: measuring the impact of malicious devices on a cellular network core. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 223–234. ACM, 2009.

[35] Ahmad Karim, Syed Adeel Ali Shah, and Rosli Salleh. Mobile botnet attacks: a thematic taxonomy. In *New Perspectives in Information Systems and Technologies, Volume 2*, pages 153–164. Springer, 2014.

[36] Masood Khosroshahy, Dongyu Qiu, and Mustafa K Mehmet Ali. Botnets in 4g cellular networks: Platforms to launch ddos attacks against the air interface. In *2013 international conference on selected topics in mobile and wireless networking (MoWNeT)*, pages 30–35. IEEE, 2013.

[37] Christian Szongott, Benjamin Henne, and Matthew Smith. Evaluating the threat of epidemic mobile malware. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on*, pages 443–450. IEEE, 2012.

[38] Gokce Gorbil, Omer H Abdelrahman, and Erol Gelenbe. Storms in mobile networks. In *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks*, pages 119–126, 2014.

[39] Alessio Merlo, Mauro Migliardi, Nicola Gobbo, Francesco Palmieri, and Aniello Castiglione. A denial of service attack to umts networks using sim-less devices. *IEEE Transactions on Dependable and Secure Computing*, 11(3):280–291, 2014.

[40] Asem Kitana, Issa Traore, and Isaac Woungang. Impact study of a mobile botnet over lte networks. *Journal of Internet Services and Information Security (JISIS)*, 6(2):1–22, May 2016.

[41] Asem Kitana, Issa Traore, and Isaac Woungang. Impact of base transceiver station selection mechanisms on a mobile botnet over a lte network. In *11th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, Puerto Rico, USA*, pages 1–9. IEEE, 2016.

[42] Asem Kitana, Issa Traore, and Isaac Woungang. Towards an epidemic sms-based cellular botnet. *Journal of Internet Services and Information Security (JISIS)*, 10(4):38–58, November 2020.

[43] Siyuan Liu, Yunhuai Liu, Lionel M Ni, Jianping Fan, and Minglu Li. Towards mobility-based clustering. In *Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 919–928. ACM, 2010.

[44] Lte technology 3gpp. `http://www.3gpp.org/technologies/keywords-acronyms/98-lte`. (Last visited December 9, 2020).

[45] Rate of lte deployment increasing report, gsa press release. http://www.3gpp.org/news-events/partners-news/1561-rate-of-lte-deployment-increasing.

[46] Bandwidth support in lte standards, qualcomm. https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting71612/panel2.3-gaal-qualcomm.pdf.

[47] 3gpp ts 24.007 mobile radio interface signalling layer 3; general aspects, rel. 11, section 11.2.3.1.5, june 2012. http://www.3gpp.org/dynareport/24007.htm.

[48] Riverbed modeler. http://www.riverbed.com/products/performance-managementcontrol/ network-performance-management/network-simulation.html.

[49] 3gpp ts 23.401, lte general packet radio service (gprs) enhancements for evolved universal terrestrial radio access network (e-utran) access, release 11. http://www.3gpp.org/dynareport/23401.htm.

[50] D. Evans, J. Groves, and W. Croft. Operator group ranking, q2 2014, chinese carriers dominate global operator ranking as m&a deals shake up us market. https://www.gsmaintelligence.com/research/2014/09/operator-group-ranking-q2-2014/444/l/.

[51] 3gpp ts 36.133, evolved universal terrestrial radio access (e-utra); requirements for support of radio resource management, release 11, september 2012. http://www.3gpp.org/dynareport/36133.htm.

[52] Shanghai jiao tong university. suvnet-trace data. http://wirelesslab.sjtu.edu.cn.

[53] Yajin Zhou and Xuxian Jiang. Dissecting android malware: Characterization and evolution. In *Proc. of the 33rd annual IEEE Symposium on Security and Privacy, San Francisco, CA, USA*, pages 95–109, May 20-23 2012.

[54] Mandana Bekhouri and Ronit Nossenson. Application benchmark for cellular backhaul network. In *Proc. of the 11th International Conference on Wireless and Mobile Communications (ICWMC 2015), St. Julians, Malta*, pages 51–56, October 11-16 2015.

[55] Ketki Arora, Krishan Kumar, and Monika Sachdeva. Characterizing ddos attack distributions from emulation based experiments on deter testbed. In *Advanced Computing, Networking and Security, Springer*, volume 7135 of *Lecture Notes in Computer Science*.

[56] Steelcentral network performance management. riverbed modeler. riverbed. https://www.riverbed.com/gb/.

[57] Riverbed modeler. riverbed lte module. https://www.riverbed.com/gb/products/all-products.html.

[58] The impact of sms on email open rates report. https://www.smsglobal.com/blog/the-impact-of-sms-on-email-open-rates/.

[59] igraph.wikidot.com. http://igraph.wikidot.com/.

[60] igraph-the network analysis tool. https://igraph.org/.