Impact of Base Transceiver Station Selection Mechanisms on a Mobile Botnet over a LTE Network

Asem Kitana
University of Victoria
Dept. of Electrical & Computer Eng.
Victoria, BC, Canada
akitana@uvic.ca

Issa Traore
University of Victoria
Dept. of Electrical & Computer Eng.
Victoria, BC, Canada
itraore@ece.uvic.ca

Isaac Woungang
Ryerson University
Dept. of Computer Science
Toronto, ON, Canada
iwoungan@scs.ryerson.ca

Abstract

This paper studies 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 on a Long Term Evolution (LTE) network. Simulation results using the Riverbed Modeller 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 of the mobile botnet on the victim server, from 100% to 70%.

1. Introduction

The rapid development of telecommunication system standards has led to the deployment of Long Term Evolution (LTE) technology (also referred to as 4G cellular networks) to overcome the increasing demand from the mobile users for reduced transmission latency, data rate and high quality of service (QoS). However, these advantages of LTE also come with serious security drawbacks as various types of cyberattacks using mobile devices can be launched on these systems. An example of such attack is the mobile botnet, a group of infected mobile devices (also called bots) that are controlled by a master attacker (also called botmaster) to achieve some harmful activities and attacks through the Command and Control (C&C) channels, the botnet threats which have been targeted primarily at stationary devices, have now expanded to mobile devices [1]. Understanding of the behavior of a mobile botnet on a LTE network in the presence is still an open problem. In this paper, the impact of two base transceiver station selection mechanisms, namely, the DBM and SPBM mechanisms, on a mobile botnet launching a DDoS attack on a LTE network involving 400 Android mobile devices is investigated using the Riverbed Modeller [2]. In the former, the selection of a suitable eNodeB station to serve the mobile devices' requests is based on the shortest distance metric whereas in the later, the same selection is based on the strongest signal power.

The rest of the paper is organized as follows. In Section 2, some related work are discussed. In Section 3, the considered LTE network architecture is presented. In Section 4, the SPBM and DBM mechanisms are described. In Section 5, the proposed mobile botnet architecture is described. In Section 6, the simulation results are presented. Section 7 concludes the paper.

2 Related Work

Various aspects of mobile botnets have been investigated in the literature. Representative works are as follows. In [3], Singh et al. demonstrated by experiments that the bluetooth technology can be used as C&C channel in a mobile botnet. In their experiments, two datasets of real traces of mobile devices are used for studying and analyzing malware propagation in a mobile botnet, leading to the design of a protection mechanism assuming that the malware binary files are accessible.

In [4], Li et al. proposed a bluetooth-based malware proximity-based infection model that uses the so-called coping structure to enable the deployment of the malware dissemination and the so-called long-term evaluation structure to control the vulnerability level of each node in the network.

In [5], Geng et al. designed an heterogeneous mobile botnet architecture and its associated infection mechanism that consists of deploying SMS messages in a C&C channel. An encryption algorithm is also implemented to conceal the malware commands and a failure/recovery mechanism is implemented at the bot servers level.

In [6], Hua and Sakurai proposed a mobile botnet architecture and two associated malware dissemination mechanisms, one that consists of deploying SMS messages in a C&C channel and the other that consists of deploying a bluetooth service in combination with a self similar least action walk model and a static mobility model.

In [7], Zhuo et al. studied the effect of the movement of mobile devices on a botnet propagation, leading to the design of a malware propagation model. By studying the epidemic propagation behavior of its proximity infection, they showed that there is an exponential decay in the mobile botnet size when the mobility radius is not large enough.

In [8], Traynor et al. studied the effect of deploying a mobile botnet that initiates a DoS attack against the home location register services of a GSM cellular network. In their experiments, the infection process is deployed using various malware propagation channels such as voice, bluetooth, and SMS messages, showing that there is a significant reduction in the service throughput of the GSM network as per the number of infected devices.

In [9], a survey of mobile botnet attacks is proposed, and different categories of mobile botnets and their associated attack vectors are investigated and classified.

Unlike previous works on mobile botnet, this paper focuses on analyzing the impact of two base transceiver station selection mechanisms on a mobile botnet that deploys a DDoS attack on a LTE network.

3 Proposed LTE Infrastructure Cellular Network

The proposed mobile botnet is considered as an overlay network that operates over an LTE network as infrastructure network, itself designed based on the 3GPP standards [10]. 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 several interfaces as shown in Fig. 1. Each of these components consists of different stacks and levels as illustrated in Fig. 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.

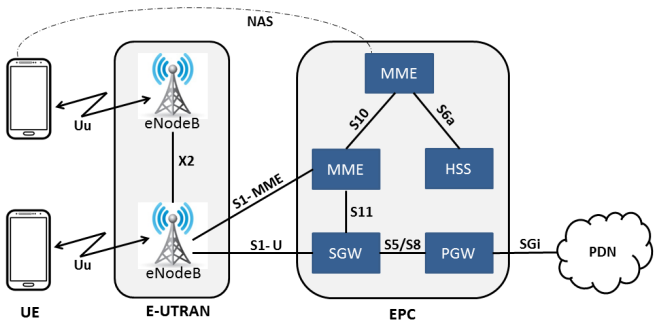

Figure 1: EPS architecture [10]

The proposed LTE network is deployed according to the LTE model implemented in the Riverbed Modeller [2], 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 default one called non-guaranteed bit rate (Non-GBR) - used to manage the traffic connection between the http application and the web server in the mobile botnet - and the dedicated one called guaranteed bit rate (GBR) bearer - used to manage the video streaming application traffic of the web server as illustrated in Fig. 2. In this setting, only two QoS Class Identifier (QCI) values, namely QCI-2 and QCI-8) have been considered from the standardized table of 3GPP TS 23.203 [10]. 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.

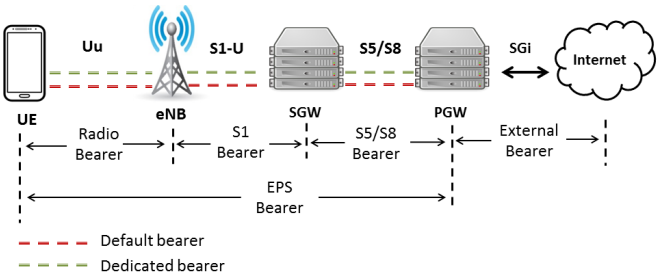

Figure 2: GBR and non-GBR EPS bearers of the considered LTE network.

The activation/deactivation mechanism of the EPS bearers is implemented according to the 3GPP standard [11]. Typically, a mobile device initiates an EPS

bearer creation by dispatching an EPS session management (ESM) bearer resource modification request [11] 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 in 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 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 [10].

Table 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: Any request for a GBR radio bearer from the eNodeB should go through this procedure. When accepted, this procedure allocates and reserves the required cell resources for this 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 allocated only if the required cell resources are available and can be assigned to the uplink and downlink directions. Otherwise, the request will be rejected. In our settings, in the admission control procedure, the preemption procedure 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, an integer in the range 1 to 15. Low ARP values corresponds 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. 3: (1) the eNodeB stack through signalling messages that are written by using the RRC protocol, and (2) the Mobility Management Entity (MME) stack through some signalling messages written by using the EPS mobility management (EMM) protocol [10]. A mobile device can switch from one EMM state [10] to another when certain traffic conditions occur; for instance, when a tracking area update is needed or when there is a traffic that should be delivered from/to the core network.

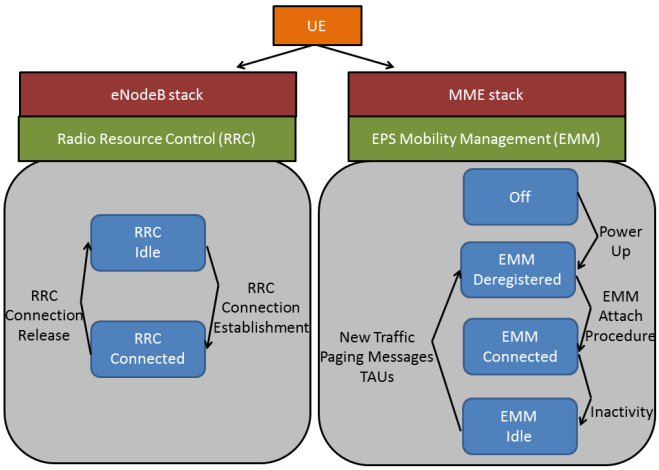

Figure 3: Mobile device control mechanism

- Physical layer deployment: It works in both the Frequency Division Duplex (FDD) and the Time Division Duplex (TDD) modes [10]. 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

Table 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 [11].
EMM_Idle	When a mobile device has no activity in the LTE network and cannot save a considerable amount of its power.

Table 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.

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 number of resource blocks [10]. 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 3.

4 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 a eNodeB station (referred to as serving eNodeB) must be selected and the UE must be connected to it. In this paper, 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). We present these two selection mechanisms in this section.

4.1 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 EPC 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 [11]. 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 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 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 [11] as done in the DBM mode, and this is based on the RSRP indicators. 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:

$$P_R = T_t \times N_t \times \left(\frac{W^2}{16\Pi^2 d^2}\right) \times N_r \qquad (1)$$

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.

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, 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: 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

For comparison purpose, the MTP values given in Table 4 are also assigned to the eNodeB stations in the DBM mode.

In the SPBM mode, the eNodeB station is responsible for triggering and managing the handover procedure as described in [11]. 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, where 4 eNodeB stations are considered, namely, eNB1, eNB2, eNB3, and eNB4, each having its own signal power strength measured in β units.

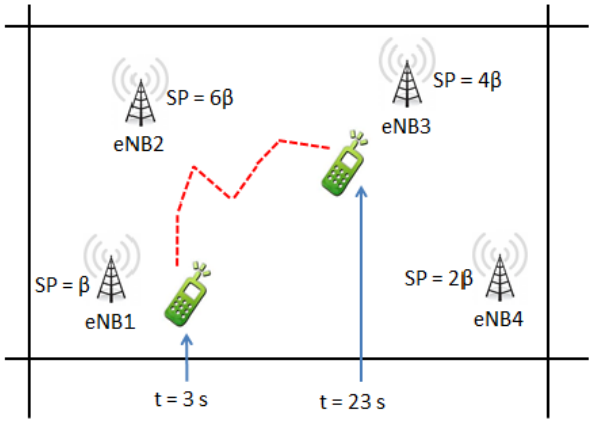

Figure 4: DBM vs. SPBM

In Fig. 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 $t = 23$ seconds, the mobile node will be connected to eNB3 in the DBM mode and to eNB2 in the SPBM mode.

5 Mobile Botnet Topology

5.1 Mobility Model

The trajectories of the movement of the mobile devices is simulated by using the Random WayPoint (RWP) model

of the Riverbed Modeller. At the start of the simulation, the RWP profile is configured in each mobile device, and each device moves according to its trajectory fragments from one destination point to another. The considered RWP profile configuration attributes are given in Table 5.

Table 5: 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

5.2 Mobile Botnet Architecture

The considered mobile botnet architecture is composed of a botmaster, the C&C server, and the LTE network as shown in Fig. 5.

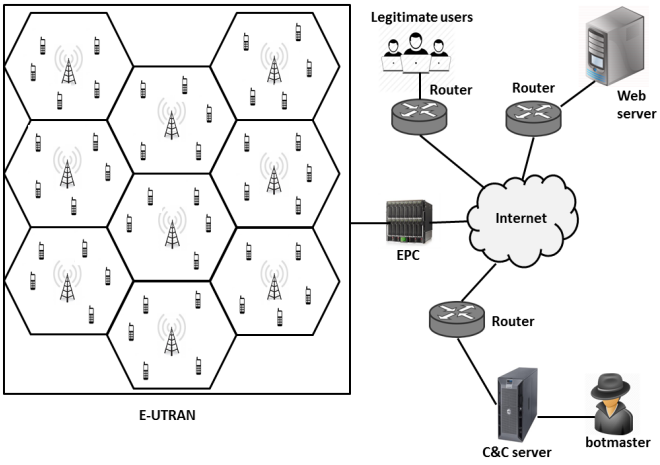

Figure 5: Mobile botnet architecture.

The botmaster is responsible for managing all the mobile botnet operations through controlling the C&C server. This server is used as gateway for the botmaster to access the infected mobile devices and deliver the 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: the DBM scenario where 400 Android mobile devices in the LTE network are allowed to be connected to their serving eNodeB stations based on the DBM mode and the SPBM scenario where the connections are operated according to the SPBM mode. In addition, an infection rate I_{MB} in the mobile botnet is defined as $I_{MB} = B_d/N_d$, where B_d is the number of bot-infected mobile devices and N_d is the total number of mobile devices.

- For $I_{MB} = 0.8$, $B_d = 340$ (case of DBM) and $B_d = 290$ (case of SPBM).
- For $I_{MB} = 0.5$, $B_d = 220$ (case of DBM) and $B_d = 170$ (case of SPBM).
- For $I_{MB} = 0.2$, $B_d = 100$ (case of DBM) and $B_d = 50$ (case of SPBM).

The functionality of the mobile botnet is executed through four main stages as per Table 6.

Table 6: 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.

5.3 Attack Model

A DDoS attack model is initiated against the victim web server as shown in Fig. 6.

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 [12]. A report is then sent

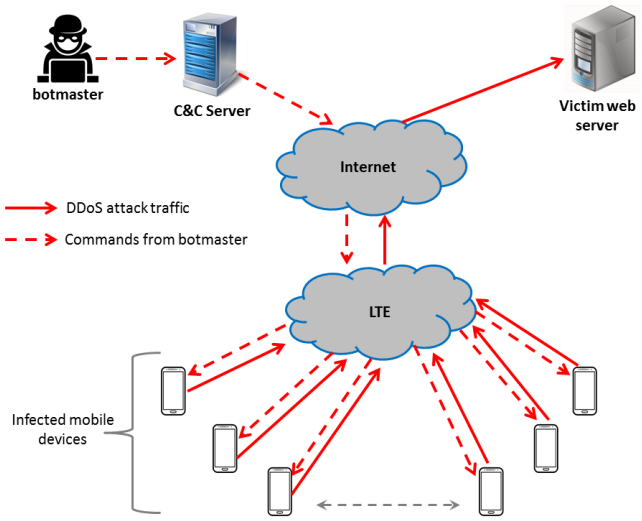

Figure 6: DDoS attack model.

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 e-commerce 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 [2] 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 [13], considering an inter arrival time of 3 milliseconds.

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 E-commerce 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 as shown in Fig. 7. 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. Algorithm 1 describes the flooding algorithm executed by the C&C server to conduct the DDoS attack.

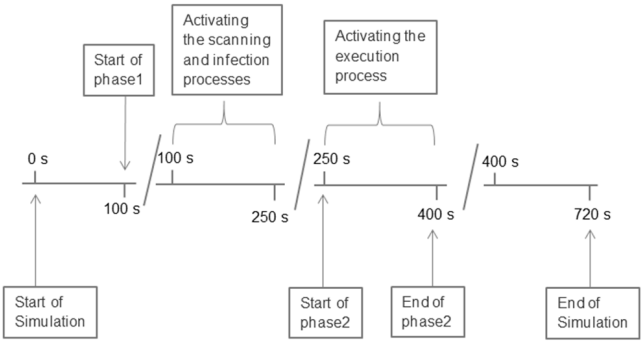

Figure 7: DDoS attack timeline

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

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

6 Simulation Results

For the considered DBM and SPBM scenarios, the same LTE network configuration features given in Table 7 have been considered.

First, the number of infected mobile devices is investigated when using the DBM vs. the SPBM scenarios. The results are summarized in Fig. 8, 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

Table 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
I_{MB}	0.8

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.

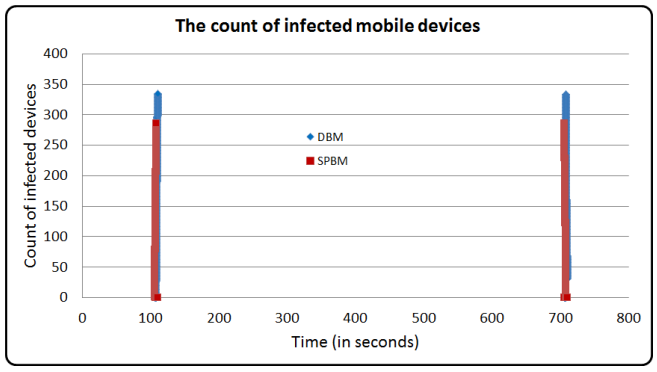

Figure 8: Number of infected mobile devices when for DBM vs. SPBM.

Second, the CPU utilization of the victim web server is measured when using the DBM vs. the SPBM scenarios. The results are captured in Fig. 9, 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.

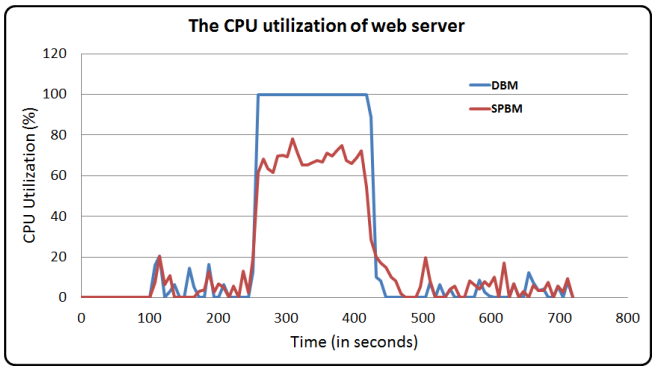

Figure 9: CPU utilization for DBM vs. SPBM.

Third, Fig. 10 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.

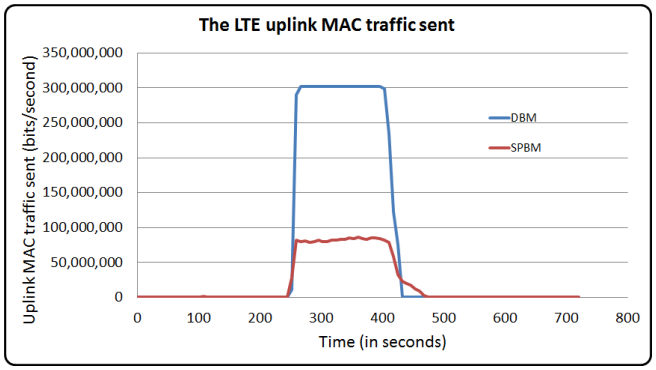

Figure 10: LTE uplink MAC traffic for DBM vs. SPBM.

Fourth, Fig. 11 captures the uplink throughput of all eNodeB stations in the LTE network when using DBM compared to using SPBM. It is observed that uplink throughput of the eNodeB stations under the DDoS attack is much higher when using DBM compared to using SPBM.

Fifth, 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. 12. It is observed that the DBM scenario consumes higher load on the victim web server compared to the SPBM scenario.

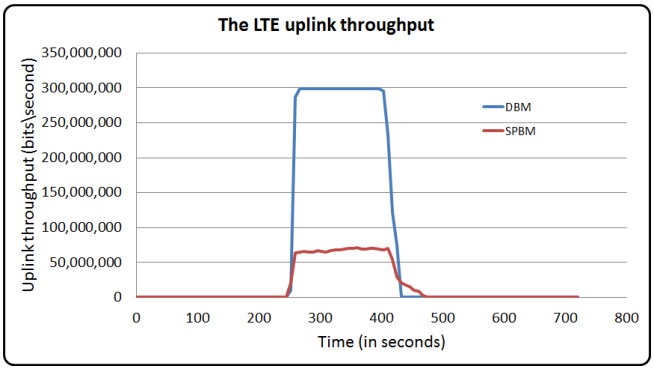

Figure 11: Uplink throughput for DBM vs. SPBM.

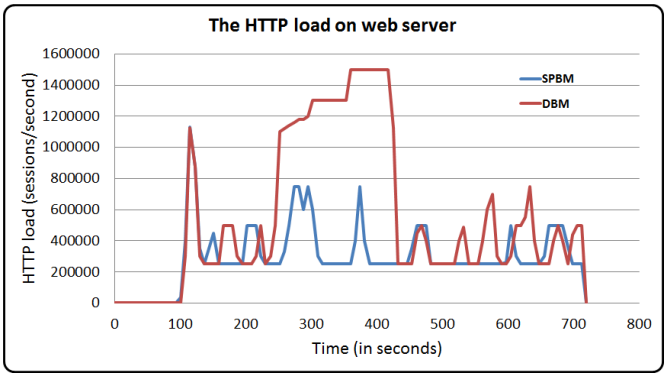

Figure 12: http traffic load for DBM vs. SPBM.

7 Conclusion

This paper 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 future work, we intend to design a baseline technique for detecting the mobile botnet and studying its behavior on the LTE network.

References

[1] B. Kitts , J. Y. Zhang, G. Wu, W. Brandi, J. Beasley, K. Morrill, J. Ettedgui, S. Siddhartha, H. Yuan, F. Gao, P. Azo, R. Mahato, "Click Fraud Detection: Adversarial Pattern Recognition over 5 Years at Microsoft", Real World Data Mining Applications, Vol. 17, Annals of Information Systems, 2015, pp 181-201.

[2] Riverbed modeler, http://www.riverbed.com/products/performance-managementcontrol/network-performance-management/network-simulation.html (Last accessed June 21, 2016).

[3] K. Singh, S. Sangal, N. Jain, P. Traynor, W. Lee, "Evaluating bluetooth as a medium for botnet command and control", Chapter in Book "Detection of Intrusions and Malware, and Vulnerability Assessment", vol. 6201, LNCS, Springer, 2010, pp. 61-80.

[4] F. Li, Y. Yang, J. Wu, "CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-based Mobile Networks", Proc. of IEEE INFOCOM 2010, San Diego, CA, USA, Mar. 15-19, 2010, pp. 1-9.

[5] G. Geng, G. Xu, M. Zhang, Y. Guo, G. Yang, C. Wei, "The design of SMS based heterogeneous mobile botnet", Journal of Computers, vol. 7, no. 1, 2012, pp. 235-243.

[6] J. Hua and K. Sakurai, "Botnet command and control based on Short Message Service and human mobility", Computer Networks, vol. 57, no. 2, 2013, pp. 579-597.

[7] L. Zhuo, W. Wenye, C. Wang, "How can botnets cause storms" Understanding the evolution and impact of mobile botnets", Proc. of IEEE INFOCOM 2014, Apr. 27-May 2, 2014, Toronto, Canada, pp. 1501-1509.

[8] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, T. La Porta, "On cellular botnets: measuring the impact of malicious devices on a cellular network core", Proc. of the 16th ACM Conference on Computer and Communications Security (CCS09), Chicago, IL, USA, 2009, pp. 223-234

[9] A. Karim, S. A. A. Shah, R. Salleh, "Mobile botnet attacks: a thematic taxonomy", New Perspectives in Information Systems and Technologies, Springer, vol. 2, 2014, pp. 153-164.

[10] LTE-A 3GPP, http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced (Last accessed June 22, 2016).

[11] 3GPP TS 23.401 , "Dedicated Bearer Activation Procedure in 3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, Rel. 11, Sept. 2012", http://www.3gpp.org/DynaReport/23401.htm (Last visited June 22, 2016).

[12] Y. Zhou, X. Jiang, "Dissecting android malware: Characterization and evolution", Proc. of the IEEE Symposium on Security and Privacy, San Francisco, USA, May 20-23, 2012, pp. 95-109

[13] K. Arora, K. Kumar, M. Sachdeva, "Characterizing DDoS attack distributions from emulation based experiments on DETER testbed", Advanced Computing, Networking and Security, Springer, Vol. 7135, Lecture Notes in Computer Science, 2012, pp. 541-550.