Towards an Epidemic SMS-based Cellular Botnet

Asem Kitana[1]*, Issa Traore[1], and Isaac Woungang[2]
[1]Department of Electrical and Computer Engineering
University of Victoria, Victoria, BC, Canada
akitana@uvic.ca, itraore@ece.uvic.ca
[2]Department of Computer Science
Ryerson University, Toronto, ON, Canada
iwoungan@scs.ryerson.ca

Abstract

Attacks and threats against cellular devices such as botnets are becoming more and more prominent. Focusing on short message services (SMS) phishing attacks, this paper proposes 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). Simulation results show that: (1) Compared to BAT and WST, ERT is the best topology for enhancing the epidemic behavior of the proposed cellular botnet, (2) the BAT topology is less resilient to devices' failures compared to the ERT and WST topologies. In the end, an effective holistic multi-tier defense strategy against the proposed epidemic SMS-based cellular botnet is presented.

Keywords: Cellular botnet, Mobile botnet, Epidemic Command and Control, C&C channel, SMS, Short Message Service, Malware

1 Introduction

The massive growth in popularity and dependence on smart phones has made them the target of different kinds of cyber-attacks. In this regard, one of the current arising cellular-based security threats is the cellular botnet [12].

A cellular botnet is a set of compromised cellular devices, also known as bots or zombies, which are controlled by a botmaster through a control mechanism known as Command and Control channels. The control of the compromised devices can be achieved by using a malware such as a malicious command injected in a short message service (i.e. malicious SMS). The capability of controlling a large group of cellular devices by a botmaster, provides acute abilities for initiating destructive and harmful cyber-attacks [19] [11].

Unlike the traditional botnets which rely on stationary devices such as desktop computers, cellular botnets rely on hand-held and cellular devices. They represent a serious security threat today and limited research have been done on investigating their behaviors. This paper presents the design of an epidemic SMS-based cellular botnet in which the C&C channel is implemented by developing an epidemic flooding algorithm (i.e. rapid and stealthy flooding algorithm). The epidemic flooding algorithm represents the core of our cellular botnet that initiates the malware propagation.

Furthermore, we have chosen three random graphs models, namely, Barabasi–and-Albert topology (BAT), Erdos-and-Reyni topology (ERT), and Watts-and-Strogatz topology (WST), to be implemented as the

Journal of Internet Services and Information Security (JISIS), volume: 10, number: 4 (November 2020), pp. 38-58
DOI: *10.22667/JISIS.2020.11.30.038*

*Corresponding author: Department of Electrical and Computer Engineering University of Victoria, P.O. Box 1700, STN CSC, Victoria, BC V8W 2Y2, Canada, Tel: +1-(250) 721.86.97

topology models for our proposed epidemic SMS-based cellular botnet. The simulation of the epidemic SMS-based cellular botnet, and the three topology models have been deployed by using the R packages of the igraph network analysis software.
This study shows that by selecting a seed (C&C server) as the hub cdevice and the most central neighbors as the receivers of the malware commands in every propagation cycle, then the Erdos-and-Renyi topology (ERT) is the optimal random graph model for our proposed epidemic SMS-based cellular botnet. The study also shows that the BAT topology is the best model for mitigating the epidemic behavior of the presented cellular botnet. By applying the ERT and BAT models, using 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. Under the above configuration a malicious SMS can be propagated to 96% of the vulnerable cdevices in the network within 9 minutes in the case of the ERT model, and to 77% of the vulnerable cdevices in the network within 9 minutes in the case of the BAT model, which makes the BAT model reduces the impact of the epidemic behavior of cellular botnets, and enhances the probability of detecting such malicious networks. Also, 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, and less robust in the case of the BAT model.
The rest of the paper is organized as follows. Section 2 discusses related work. Section 3 discusses the challenging issues of our work. Section 4 presents our proposed epidemic flooding algorithm, followed in Section 5 by an analysis of it. In Section 6, simulation results are presented. Section 7 discusses the proposed defense strategy against the epidemic cellular botnet. Finally, Section 8 concludes the paper.

2 Related Work

While mobile botnet is an emerging field of research, a few proposals have been published in addressing various aspects of the threat. In [16], Singh et al. performed two experiments to demonstrate the ability of using bluetooth technology as C&C channel for conducting the malware propagation in a mobile botnet. Zeng et al. [20] studied the malware infection mechanism in a mobile botnet by using SMS messages as propagation mechanism. In their study, a word mapping technique was deployed to enhance the efficiency of their propagation mechanism.
Li et al. [13] proposed a bluetooth-based malware infection mechanism that relies on proximity between nodes, contact history, and network grouping structure. In [6], Geng et al. proposed a SMS-based malware infection mechanism by using a multi-tree network topology. However, their proposed model completely relies on theory without providing any implementation or simulation experiments.
Hua and Sakurai [8] proposed two malware propagation techniques in a mobile botnet. The first technique is a SMS-based mechanism, while the second technique is a bluetooth-based mechanism.
Zhuo et al. [14] proposed a malware propagation mechanism in a mobile botnet by using a stochastic model. The result of their study showed that there is a quadratic relationship between the average size of a mobile botnet and its mobility range.
In [18], Traynor et al. proposed a mobile botnet that initiates a DoS attack against the Home Location Register (HLR) services of a GSM network. In [9], Karim et al. conducted a comprehensive review on mobile botnet attacks by investigating the different categories of mobile botnets and their attack vectors. A state-of-the-art comparison between different authors for the cellular botnet construction is conducted in Table 1. While in Table 2, a comparison between our proposed epidemic SMS-based cellular botnet model and Hua-Sakurai model is presented.

Table 1: State-of-the-art comparison between different authors for the cellular botnet construction.

Author	**C&C Mechanism**	**Attack Model**	**Simulation Tool**
Singh et al. [16]	Bluetooth	DoS attack	Sun Wireless Toolkit
Gorbil et al. [7]	UMTS	DCH/FACH attacks	OMNeT++
Zeng et al. [20]	SMS messages	Flooding attack	OverSim
Khosroshahy et al. [10]	LTE	DDoS attack	LTESim Framework
Hua et al. [8]	Bluetooth and SMS messages	SMS phishing	NS-2 and iGraph
Li et al. [13]	Bluetooth	Flooding attack	Trace-driven
Zhuo et al. [14]	Bluetooth	DoS attack	UDelModels
Kitana et al. [12]	LTE	DDoS attack	Riverbed Modeler
Traynor et al. [18]	GSM	DoS attack	Telecom One (TM1)
Merlo et al. [15]	UMTS	DoS attack	SIM-less device
Geng et al. [6]	SMS messages	Flooding attack	Math analysis
Szongott et al. [17]	WiFi	Evil Twin attack	Mobile Security and Privacy Toolkit
Proposed epidemic cellular botnet	SMS messages	SMS phishing	iGraph

Table 2: Hua-Sakurai model vs. Proposed model.

Parameter	**Hua-Sakurai Model**	**Proposed 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

3 Challenging issues

Like the traditional botnet networks, a cellular botnet network relies on the Command and Control (C&C) channel, which represents the core component of the cellular botnet. Therefore, an efficient cellular bot-

net employs an epidemic C&C channel. A C&C channel should have two characteristics to be defined as epidemic, which are, Speed and Stealth. The speed characteristic of the C&C channel refers to the ability of the botmaster through the C&C channel to propagate the malware to a vast amount of susceptible cellular phone devices in a short time. The stealth characteristic of the C&C channel refers to the ability of disseminating the malware in a concealed manner so that cellular phone users cannot detect the malware propagation mechanism. Therefore, in this paper, we have considered the aforementioned characteristics of the epidemic C&C channel (speed and stealth) in designing the proposed epidemic cellular botnet. The architecture of our proposed cellular botnet is implemented by leveraging the SMS mechanism as C&C channel, which is a low cost service available in all the cellular phone devices. In the design of our proposed epidemic SMS-based cellular botnet, there is a dilemma, that is represented by the discrepancy of rapidly propagating the malicious commands to a large number of susceptible cellular phone devices in the network, and the deployment of 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 phone devices in the network in a short period of time, the group-messaging mechanism should be applied. This contradicts the concept of a stealthy C&C channel because the group-messaging mechanism facilitates the detection of the malicious SMS and C&C channel behavior by the end users. Therefore, the main challenge in our proposed epidemic SMS-based cellular botnet design is how to deploy an epidemic C&C channel that can quickly disseminate few malicious SMS messages in a short period of time to a large number of cellular devices while satisfying the speed characteristic?

4 Proposed Epidemic Command and Control Mechanism

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

- Figures and statistics indicate that the successful open rate of SMS is more than 98%. And out of this 98% rate, 90% of open rate occurs within 3 minutes of receiving the SMS messages by end users [3].
- SMS service doesn't rely on the Internet as 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 in 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 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 which 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 Figure 1.

In our proposed cellular botnet (Figure 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

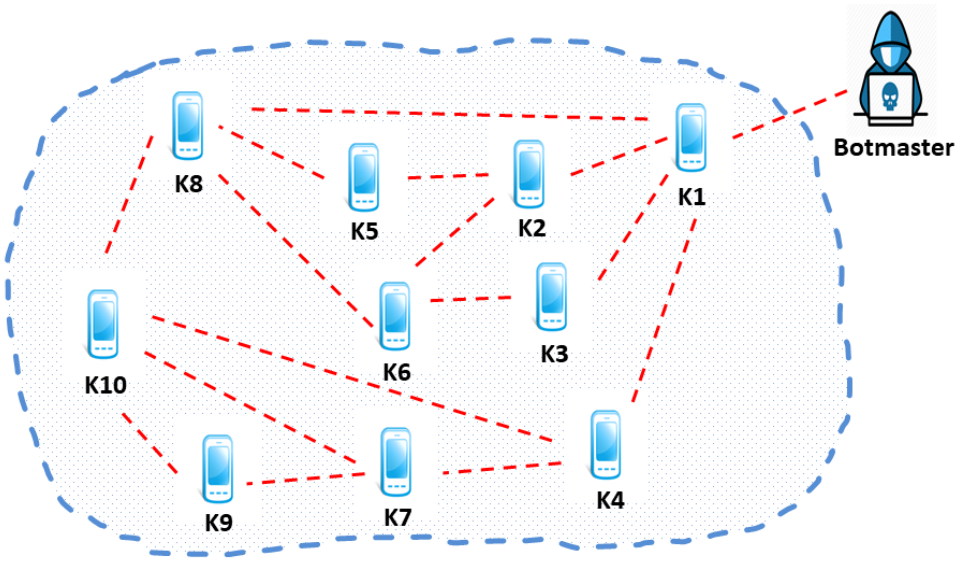

Figure 1: An epidemic SMS-based cellular botnet.

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, 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 command (malware) as 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 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 2, to regulate the malware propagation mechanism.
As shown in the sample of our proposed epidemic SMS-based cellular botnet in Figure 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 are applied to the other neighbors in the cellular botnet network.
Our epidemic flooding algorithm in Algorithm 2 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:

- 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].
- 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.
- 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.
- 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 1 will be fed as input to Algorithm 2.

Algorithm 1

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

start;
for $\forall\ i \in n\_cdevice$ **do**
    $degree\_i = \sum_{j=1}^{n\_cdevice} AMat(i,j)$
    $peers\_i = \{x \parallel AMat(i,j) = 1, \forall\ j = 1,...,n\_cdevice\}$
    cdevice_data(i, $label$) = i
    cdevice_data(i, $degree$) = $degree\_i$
    cdevice_data(i, get) = 0
    cdevice_data(i, $forward$) = 0
end for
seed = hub(1,...,*n_cdevice*)
end

Algorithm 2 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 $i = 1, ..., n\_cdevice$.

start;
cdevice_data(seed, get) = 1;
$flag = 1$;
while $flag = 1$ **do**
  for ∀ cdevice i ∈ n_cdevice **do**
    count = 0
    peer = *peers_i*
    cdevice_data_i = cdevice_data(i,:), i ∈ peer ∧ cdevice_data(i, get) = 0 ∧ cdevice_data(i, forward) = 0
    Sort cdevice_data_i, using the column degree in a descending order.
    Set n_forward as row size in cdevice_data_i.
    if n_forward = 0 **then**
      cdevice_data(i,forward) = 1
    else
      t_forward = cdevice_data(i,get)
      for ∀ s ∈ (1, min(4, n_forward)) **do**
        t_forward = t_forward + Random[60sec, 120sec]
        if t_forward ≤ t_spread + 1 **then**
          cdevice_data(cdevice_data_i (s, label), get) = t_forward
          count = count + 1
        end if
      end for
      cdevice_data(i,forward) = 1
    end if
  end for
  if count = 0 **then**
    $flag = 0$
  end if
end while
total number of infected cdevices = $\sum_{i=1}^{n\_cdevice} 1_{(cdevice\_data(i,get)>0)}$
end

5 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 $V = [n] = 1, ..., n$ for some positive integer n.

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 $i, j \in [n]$. $AMat$ 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).

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

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:

$$peers\_i = \{x \parallel AMat(i, j) = 1, \forall j = 1, ..., n\_cdevice\} \tag{2}$$

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:

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

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.

$$2m = \sum_{i=1}^{n\_cdevice} k_i = \sum_{ij} AMat(i, j) \tag{4}$$

Then the mean degree c of a cellular device

$$c = \frac{1}{n\_cdevice} \sum_{i=1}^{n\_cdevice} k_i \tag{5}$$

the mean degree c can be written as:

$$c = \frac{2m}{n\_cdevice} \tag{6}$$

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 "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).
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.

$$P_k = P(k_v = \lceil N(v) \rceil) \tag{7}$$

In this paper, we study 3 random graphs 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).
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 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 (cdevices) $V = [n] = \{v_i : i = 1,...,n\}$ is:

$$\pi(v_i) = \frac{k_{v_i}}{\sum_j k_{v_i}} \tag{8}$$

where k_{v_i} is the degree of cdevice v_i, and $\sum_j k_{v_i}$ is the total 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:

$$P_k = P(k_v = \lceil N(v) \rceil) \approx Sk^{-\alpha} \approx 2m^{1/\beta}k^{-\alpha} \tag{9}$$

where $\beta = 1/2$, and α which is the exponent of the power law $= 3$.
The ERT is a model that has n nodes, and the edge between each distinct pair of nodes is placed with an independent probability p. 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:

$$m = \binom{n}{2} p \tag{10}$$

where $\binom{n}{2}$ is the number of pairs of nodes, and p is the average 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:

$$P_k = P(k_v = \lceil N(v) \rceil) = \binom{n-1}{k} p^k (1-p)^{n-1-k} \tag{11}$$

And the average degree (k) in the ERT model is given by:

$$k = c = \left\langle \frac{2m}{n} \right\rangle = \frac{2\langle m \rangle}{n} = \frac{2}{n}\binom{n}{2} p = (n-1)p \tag{12}$$

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:

$$P_k = P(k_v = \lceil N(v) \rceil) = e^{-z}\frac{z^k}{k!} \tag{13}$$

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

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 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 $p = 0.5$.

6 Simulation Results

In this Section, our proposed epidemic SMS-based cellular botnet is evaluated using the BAT, ERT, and WST as topology for the cellular botnet network, respectively; the goal being 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.

6.1 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 the 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 among 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 2.

Figure 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 of the same and BAT which 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 3 and 4 illustrate the scenario where each cdevice in the network can forward only 3 malicious messages 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.

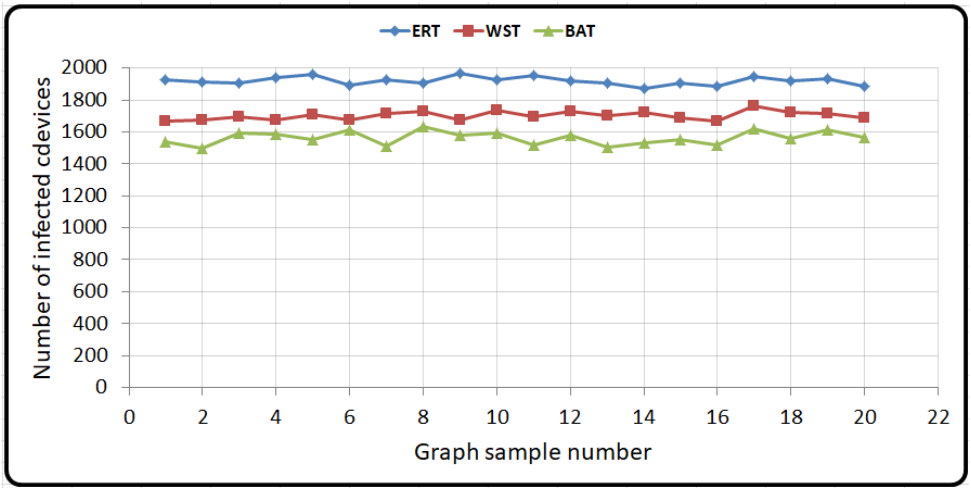

Figure 2: Forwarding Bound = 4

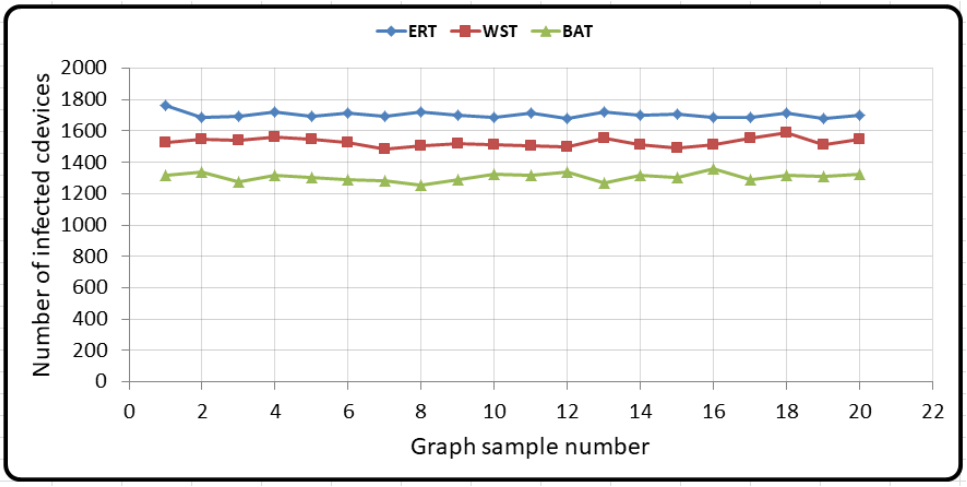

Figure 3: Forwarding Bound = 3

6.2 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.

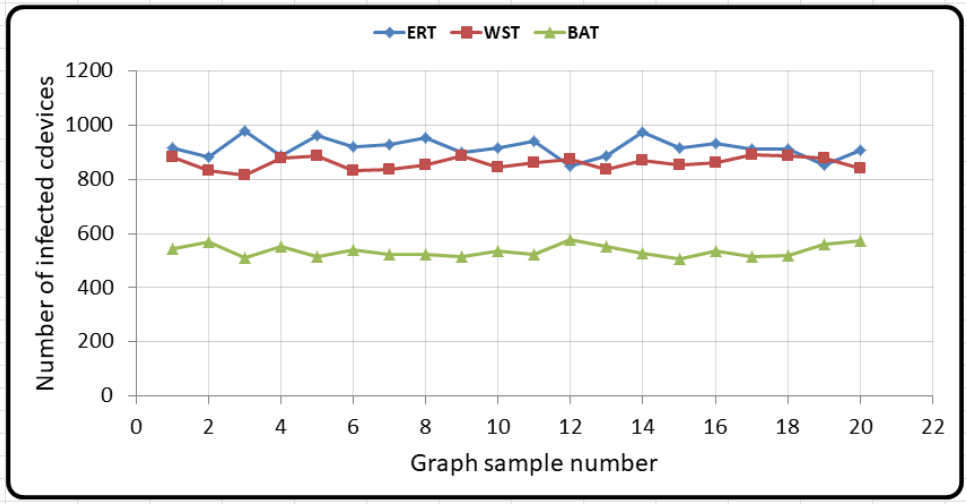

Figure 4: Forwarding Bound = 2

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, SWT, 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 rising 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. Figure 5 shows the 20 runs for the 20 ERT graph samples for each value of ACD, in terms of 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 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 7, where it is observed that the rate of infected cdevices 85% of the when ACD value is 8, 77% when the value of ACD is 6 and 48% when the ACD value is 4.

6.3 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 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 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 are 825 (for a botnet size of 1500), 650 (for a botnet size of 1000), and 400 (for a

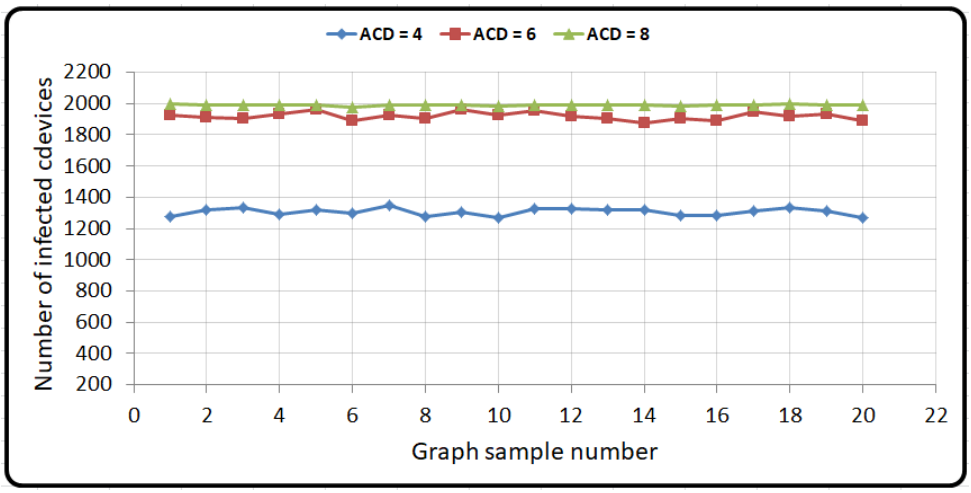

Figure 5: ACD of ERT

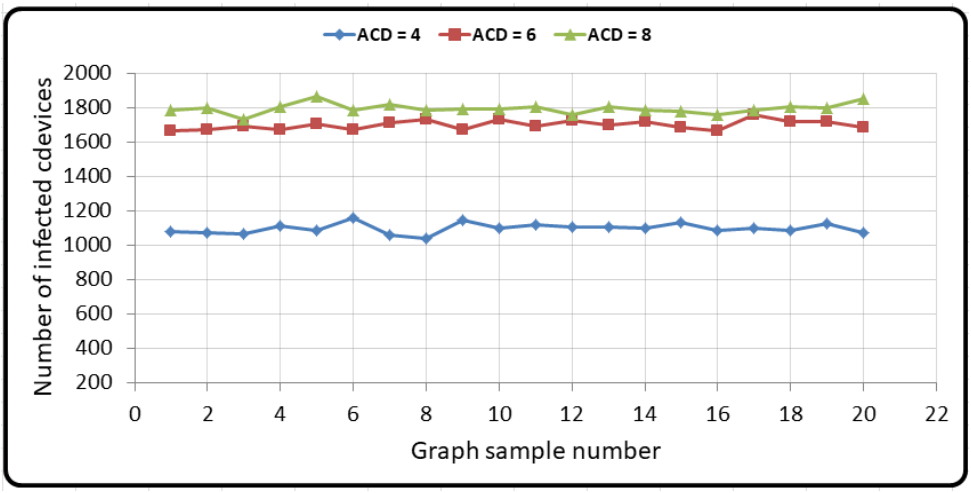

Figure 6: ACD of WST

botnet size of 500), respectively, as shown in Figure 10.

6.4 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

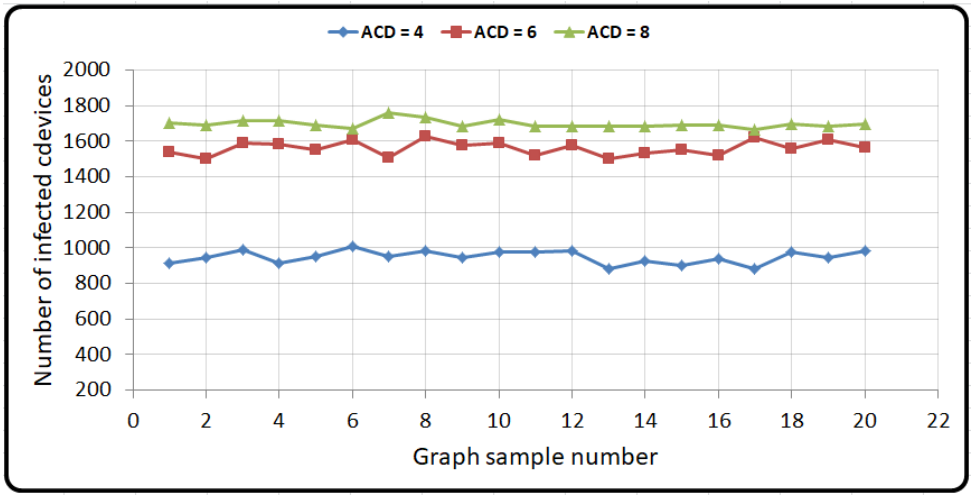

Figure 7: ACD of BAT

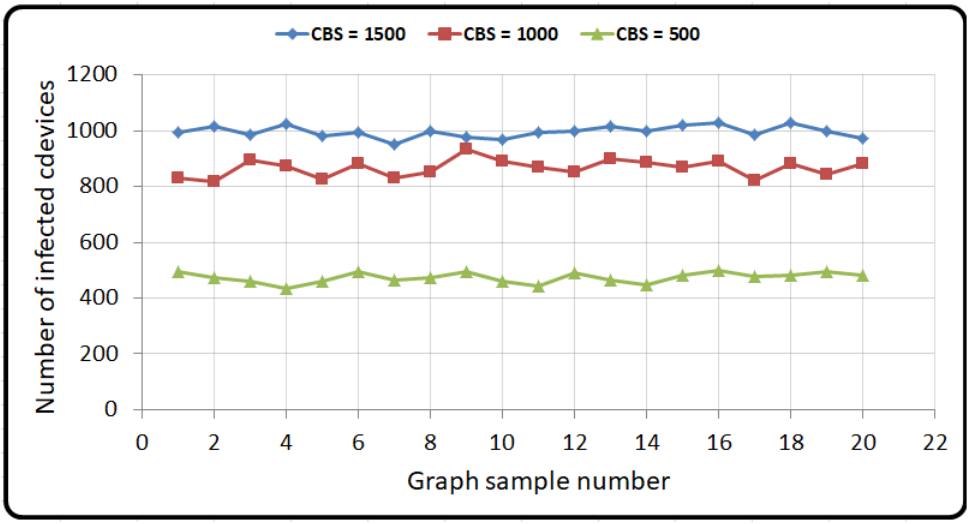

Figure 8: CBS of ERT

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 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 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 12 shows the results of running the simulation of the selective cdevice failure paradigm as shown, 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

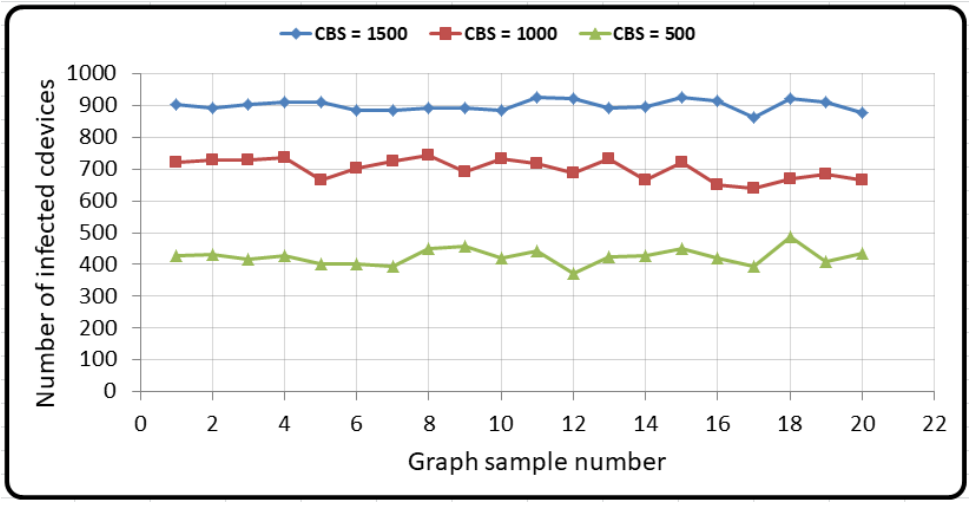

Figure 9: CBS of WST

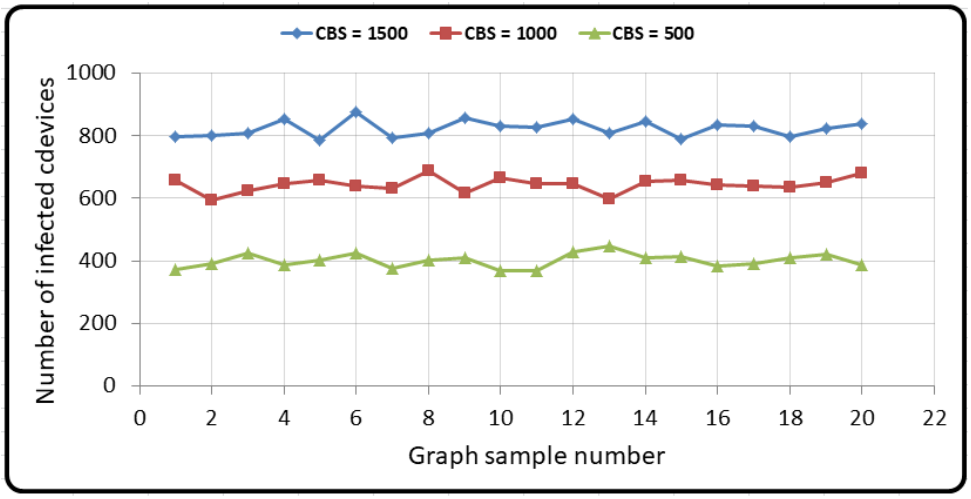

Figure 10: CBS of BAT

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 11 and 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.

7 Proposed Defense Strategy

In this section, we propose an effective strategy for protecting systems' resources and data against the epidemic behavior of our proposed SMS-based cellular botnet. Our proposed defense strategy relies on a holistic approach that operates at diverse levels, and implements different countermeasures. To properly deploy our proposed defense strategy, and put it into the most efficient functionality, a multi-tier approach is implemented, to fortify resources and data against the epidemic SMS-based cellular botnet threats.
To do so, the proposed multi-tier defense approach should consist of the following three tiers, where each

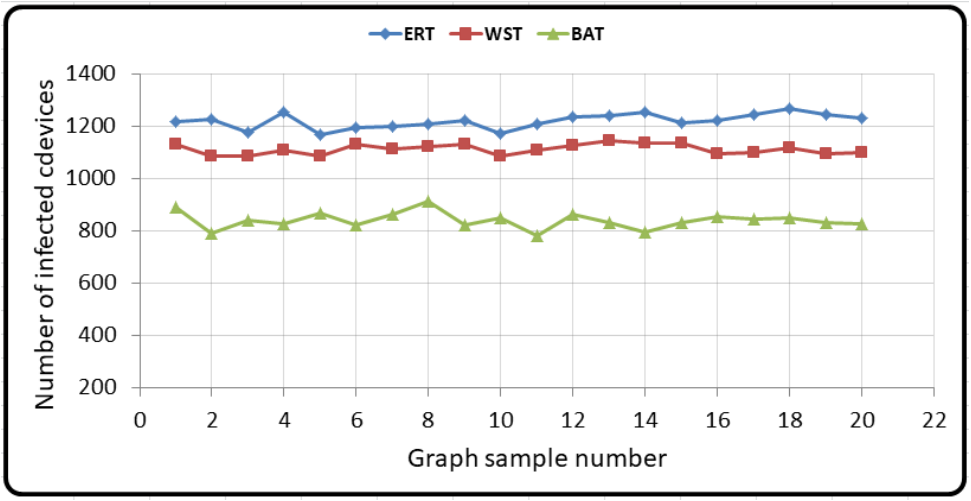

Figure 11: Random cdevice failure

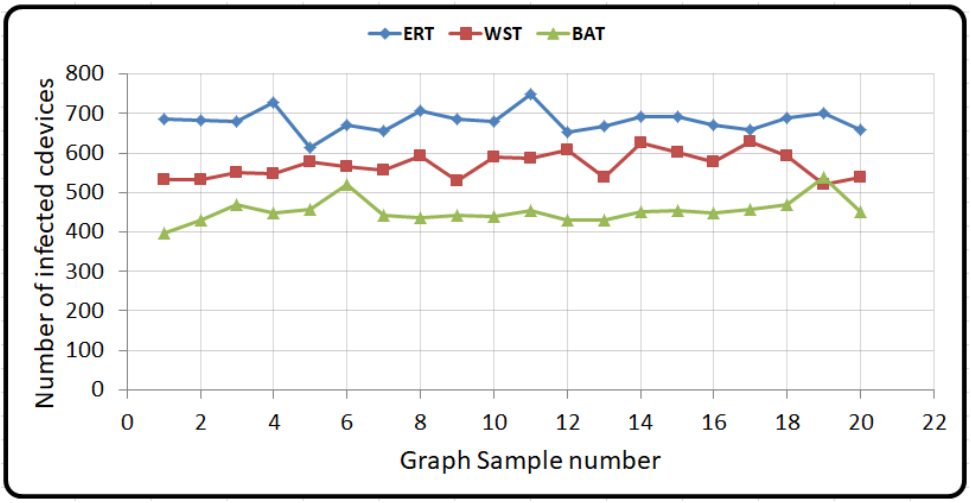

Figure 12: Selective cdevice failure

tier has its related countermeasures. Figure 13 depicts the architecture of our proposed holistic multi-tier defense approach.

7.1 The User Tier

In any cellular device, or cellular network, the user interaction (i.e. the human factor) is required for running various actions. Therefore, attackers (e.g. botmasters) noticed the significance of the human interaction in the process of finding vulnerabilities in susceptible cellular devices. Thus, different types of malware installation and activation techniques to bypass security measures rely on users' behavior, such as social engineering techniques. Social engineering is the process of employing social skills to deceive users to expose private information, so attackers (e.g. botmasters) can get access to systems (e.g. cellular devices), and installing malicious software (e.g. bot) to establish a cellular botnet.
User errors, privileges misuse, absence of security awareness sessions, lack of security training, lack of security education, and unclear commands and operations could lead to severe attacks, security breaches,

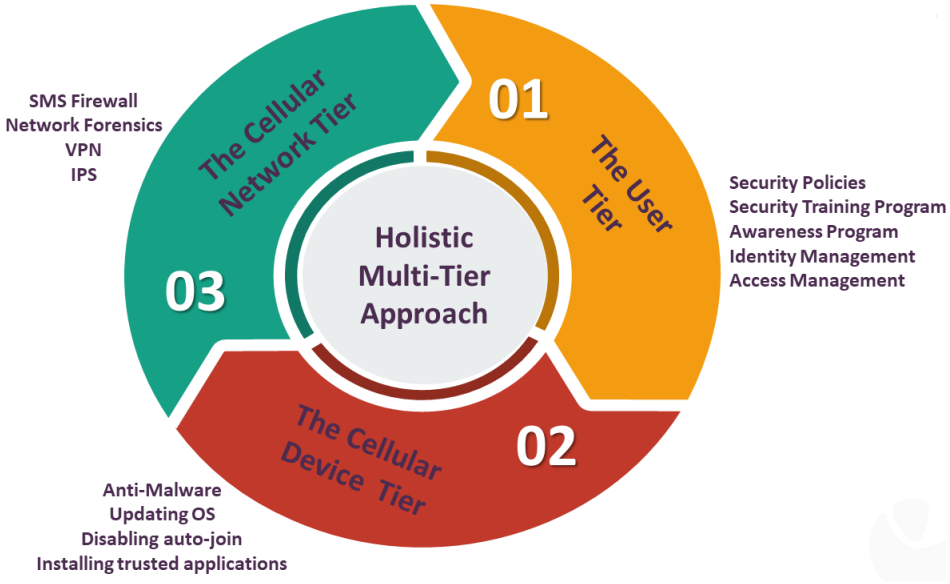

Figure 13: The holistic multi-tier defense approach

and controlling cellular devices and network. Therefore, users represent the weakest link in any defense strategy against cellular botnet.
In 2019, a study shows that 60% of cyber attacks on UK businesses have been caused by employee errors. [5] [1]. Also, in 2019, a research reveals that 90% of data breaches are caused by user errors. [4] [2]
As a result, the following countermeasures are required to improve the security posture, and protect against the risks and threats of cellular botnet.

- Applying security policies, by providing clear security guidelines, such as defining clear BYOD policies.
- Providing security awareness, training, and education programs to enhance security knowledge and skills of users.
- Defining sanctionary procedures for users who violate existing security measures, such as installing unauthorized applications in corporations.
- Deploying identity management and access management tools to prevent violating users privileges.

7.2 The Cellular Device Tier

The second level of the holistic muti-tier defense approach is protecting the cellular device itself as hardware and software against the proposed epidemic SMS-based cellular botnet. To do so, the following procedures should be deployed:

- Installing Anti-Malware tools (e.g. Anti-Virus software)
- Installing host-based intrusion prevention applications.
- Keeping cellular devices locked
- Keeping cellular devices' OS updated

– Disabling automatic-join features in cellular devices, such as auto connect WiFi networks, and auto Bluetooth pairing.

– Ignoring SMS messages that request private information, such as credentials and financial personal information.

– Installing trusted applications into cellular devices from official stores only.

– Avoiding saving sensitive information such as passwords in cellular devices. Also, avoiding clicking on links in unsolicited commercial messages.

By applying the previous procedures and techniques on cellular devices, we can protect against the risks and threats of the epidemic SMS-based cellular botnet, and enhancing the security posture of the cellular devices.

7.3 The Cellular Network Tier

The last level of the the holistic muti-tier defense approach is represented by the cellular network tier. Most of the operations, services, and activities are performed at the core components of cellular networks, which lure attackers to scan for vulnerabilities at the network level, so they can install malicious software such as mobile bot, to construct a mobile botnet. Therefore, the following techniques and mechanisms should be applied to protect against the threats of the epidemic SMS-based cellular botnet:

– Virtual Private Network (VPN):
A Virtual Private Network is a mechanism that establishes a protected channel that allows two parties to securely communicate over insecure network, such as cellular network. To protect against the epidemic behavior of the cellular botnet, a VPN mechanism that relies on the Internet Protocol Security (IPSec) architecture should be implemented. By implementing the IPSec architecture, three main security protocols are activated, namely, Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Security Association and Key Management Protocol (ISAKMP). The three security protocols provide authentication, integrity, confidentiality, and encryption security services for accessing cellular network's resources, and consequently, initiating encrypted and secure communication sessions. Therefore, VPN mechanism represents a powerful technique for enhancing the security posture of cellular networks, and protecting them from attacks and threats that are associated with the epidemic cellular botnet.

– SMS Firewall:
A firewall is a hardware device or software tool that acts as a gateway (i.e. checkpoint) between internal private networks and external insecure networks. The firewall mechanism relies on security policies that define, determine, and control what type of services to be filtered (e.g. http, ftp, smtp) and what traffic direction to be checked (i.e. ingress or egress). Therefore, network traffic can be classified as bogus traffic or genuine traffic.
A special type of firewalls is the SMS firewall. SMS Firewall protects cellular networks against malicious SMS messaging attacks, by controlling and inspecting all the SMS messages on the network. The mechanism of the SMS firewall relies on the process of routing all the SMS messages through the firewall, then analysis and classification operations are conducted to identify and block bogus messages. Thus, the implementation of SMS firewall at the cellular network side boosts the security measures of cellular networks, and establishes a shield against the threats of the epidemic cellular botnet.

– Intrusion Prevention System (IPS):
IPS is a system that automatically detect and hinder network attacks, by capturing anomalies, and protecting network resources. For instance, a common technique for propagating malware into cellular networks is conducted when users bring their own cellular devices that already infected with malware such as bot, and connect them to a corporate cellular network, in this situation, IPS can limit and block the dissemination of bot malware to other cellular devices in the cellular network. The deployment of network-based IPS reinforces the anomaly detection and network learning, by inspecting all the traffic that passes through the cellular network. Therefore, preventing the dissemination of malicious activities in the cellular network.
Network-based IPS also could be used to enhance and support the implementation of security policies, by classifying cellular network traffic based on applications. Therefore, IPS can detect, isolate, and drop unauthorized and malicious applications traffic, such as terminating the activities of epidemic SMS-based cellular botnet.

– Network Forensics:
Network forensics is the process of capturing, recording, and analyzing network events to discover the source of security attacks and incidents. Network forensics has two types, namely, Catch-it-as-you-can, and Stop, look and listen.
The deployment of network forensics systems can detect, limit, and block the malware dissemination of cellular botnet in cellular networks. To do so, after capturing packets passing through a certain traffic in the cellular network, statistical and social network analysis techniques are applied to create normal traffic profile, and then compare it with abnormal behavior. For instance, statistical anomaly detection is one of the techniques that used for detecting cellular botnet behavior by monitoring the cellular network traffic, and consequently building normal and abnormal profiles. Fuzzy techniques and Artificial Neural Network (ANN) algorithms are other approaches that could be used.

8 Conclusion

In this paper, 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 a 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 ERT model, and less resistant in the case of BAT model. Furthermore, we have proposed an effective holistic multi-tier defense strategy against our proposed epidemic SMS-based cellular botnet. The defense strategy consists of three main levels, namely, the user tier, the cellular device tier, and the cellular network tier. In each level, efficient countermeasures are presented. Our future work 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 paper 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 and 5G.

References

[1] Employee error major cyber weakness. https://www.todayslegalcyberrisk.co.uk/main-news/employee-error-major-cyber-weakness/,[Online; accessed on October 21, 2020].

[2] Human errors cyber breaches - cyber security intelligence. https://www.cybersecurityintelligence.com/blog/90-of-breaches-are-caused-by-human-error-4820.html,[Online; accessed on October 21, 2020].

[3] The impact of sms on email open rates report. https://www.smsglobal.com/blog/the-impact-of-sms-on-email-open-rates/,[Online; accessed on August 3, 2020].

[4] Meaningful metrics for human cyber risk. https://www.cybsafe.com/whitepapers/meaningful-metrics-whitepaper/, [Online; accessed on October 21, 2020].

[5] Uk businesses and cyber attacks due to employee error - information age. https://www.information-age.com/most-uk-businesses-suffered-cyber-attacks-due-employee-error-123488120/, [Online; accessed on October 21, 2020].

[6] G. Geng, G. Xu, M. Zhang, Y. Guo, G. Yang, and C. Wei. The design of sms based heterogeneous mobile botnet. *Journal of Computers*, 7(1):235–243, January 2012.

[7] G. Gorbil, O. H. Abdelrahman, and E. Gelenbe. Storms in mobile networks. In *Proc. of the 10th ACM symposium on QoS and security for wireless and mobile networks, Montréal, Québec, Canada*, pages 119–126, Septembe 2014.

[8] J. Hua and K. Sakurai. Botnet command and control based on short message service and human mobility. *Journal of Computer Networks*, 57(2):579–597, February 2013.

[9] A. Karim, S. A. A. Shah, and R. Salleh. *Mobile botnet attacks: a thematic taxonomy*. Springer, 2014.

[10] M. Khosroshahy, D. Qiu, and M. K. M. Ali. Botnets in 4g cellular networks: Platforms to launch ddos attacks against the air interface. In *Proc. of the 2013 international conference on selected topics in mobile and wireless networking (MoWNeT'13), Montréall, Québec, Canada*, pages 30–35. IEEE, August 2013.

[11] A. Kitana, I. Traore, and I. Woungang. Impact of base transceiver station selection mechanisms on a mobile botnet over a lte network. In *Proc. of the 11th International Conference on Malicious and Unwanted Software (MALWARE'11), Fajardo, Puerto Rico, USA*, pages 1–9. IEEE, October 18–21 2016.

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

[13] F. Li, Y. Yang, and J. Wu. Cpmc: An efficient proximity malware coping scheme in smartphone-based mobile networks. In *Proc. of the 29th IEEE Conference on Computer Communications (INFOCOM 2010), San Diego, California, USA*, pages 1–9. IEEE, March 14–19 2010.

[14] Z. Lu, W. Wang, and C. Wang. How can botnets cause storms? understanding the evolution and impact of mobile botnets. In *Proc. of the 33rd Annual IEEE International Conference on Computer Communications (INFOCOM'14), Toronto, Ontario, Canada*, pages 1501–1509. IEEE, April 27–May 2 2014.

[15] A. Merlo, M. Migliardi, N. Gobbo, F. Palmieri, and A. Castiglione. A denial of service attack to umts networks using sim-less devices. *IEEE Transactions on Dependable and Secure Computing*, 11(3):280–291, April 2014.

[16] K. Singh, S. Sangal, N. Jain, P. Traynor, and W. Lee. Evaluating bluetooth as a medium for botnet command and control. In *Proc. of the 7th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA'10), Bonn, Germany*, pages 61–80. IEEE, July 8–9 2010.

[17] C. Szongott, B. Henne, and M. Smith. Evaluating the threat of epidemic mobile malware. In *Proc. of the 8th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'12), Barcelona, Spain*, pages 443–450. IEEE, October 2012.

[18] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. L. Porta. On cellular botnets: measuring the impact of malicious devices on a cellular network core. In *Proc. of the 16th ACM Conference on Computer and Communications Security (CCS'09), Chicago, Illinois, USA*, pages 223–234. ACM, November 2009.

[19] C. Xiang, F. Binxing, Y. Lihua, L. Xiaoyi, and Z. Tianning. Andbot: towards advanced mobile botnets. In *Proc. of the 4th USENIX Conference on Large-scale Exploits and Emergent Threats (LEET'11), Boston,*

Massachusetts, USA, pages 11–11. ACM, March 2011.

[20] Y. Zeng, X. Hu, and K. G. Shin. How to construct a mobile botnet? In *Proc. of the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2010), Chicago, Illinois, USA*, page 2 pages. IEEE, June 28–July 1 2010.

Author Biography

Asem Kitana is a Ph.D. candidate in the Electrical and Computer Engineering Department at the University of Victoria, BC, Canada. He received his M.Sc. in Network Security from DePaul University in Chicago, USA in 2007. He has technical experience in network security technologies including Intrusion Prevention Systems, Intrusion Detection Systems, Firewall Systems, and Smart Security Solutions. He is currently a research assistant and member of the Information Security and Object Technology (ISOT) Lab at the University of Victoria (http://www.isot.ece.uvic.ca). His research interests are mobile security, Internet of Things (IoT) security, intrusion prevention systems, botnet, and malware analysis.

Issa Traore is the co-founder of Plurilock Security Solutions Inc. (www.plurilock.com) He has been with the faculty of the Electrical and Computer Engineering Department of the University of Victoria since 1999, where he is currently a Professor. Dr. Traore is also the founder and Director of the Information Security and Object Technology (ISOT) Lab (www.isot.ece.uvic.ca). He obtained in 1998 a PhD in Software Engineering from the Institute Nationale Polytechnique of Toulouse, France. His main research interests are biometrics technologies, intrusion detection systems, and software security.

Isaac Woungang is a Professor at the Department of Computer Science at Ryerson University and Director of the Distributed Applications and Broadband (DABNEL) Lab. He received his Ph.D degree in Mathematics from the University of Toulon, France, in 1994. His current research interests include network security, radio resource management in next generation wireless networks, and cloud computing. He has published 8 books and over 90 refereed technical articles in scholarly international journals and proceedings of international conferences. He has served as Associate Editor of the Computers and Electrical Engineering (Elsevier), and the International Journal of Communication Systems (Wiley). Since January 2012, He is the Chair of Computer Chapter, IEEE Toronto Section.