The Design of SMS Based Heterogeneous Mobile Botnet

Guining Geng, Guoai Xu, Miao Zhang and Yanhui Guo
Information Security Center,
Beijing University of Posts and Telecommunications, Beijing, China
gengguining@163.com, {xga, zhangmiao, yhguo }@bupt.edu.cn
Guang Yang
China Information Technology Security Evaluation Center, Beijing, China
sunwina@126.com
Wei Cui
Information Center of Ministry of Science and Technology of the People's Republic of China
cuiw@most.cn

Abstract—**Botnets have become one of the most serious security threats to the traditional Internet world. Although the mobile botnets have not yet caused major outbreaks worldwide in cellular network, but most of the traditional botnet experience can be transferred to mobile botnet on mobile devices, so mobile botnet may evolve faster since techniques are already explored. From the theoretical work of some researchers and the reports of security companies, we can see that the mobile botnet attacks and trends are quite real. In this paper, we proposed a SMS based heterogeneous mobile botnet, and shown how SMS based C&C channel structure can be exploited by mobile botnets. At last, we give the analysis of connectivity, security and robustness evaluation of our model.**

***Index Terms*—heterogeneous, mobile botnet, SMS, C&C, robustness**

I. INTRODUCTION

Traditional botnets have become one of the most serious security threats to the Internet. The word “bot” means that those victims controlled by attacker, and it derives from the word “robot”. A bot master can control a large scale of bots at different locations to initiate attack, and due to the complexity of the internet, it can be hardly trace back, and lots of researchers have done remarkable studies about the traditional botnet, such as botnet threats[1], botnet model[2], control strategies[3] and botnet detection[4].

Compared with the evolution of traditional botnet on the Internet world, mobile botnet are 7-8 years[5] behind. Although the mobile botnets have not yet caused major outbreaks worldwide in cellular network, but most of the traditional botnet experience can be transferred to mobile botnet. Norman[5] predicts that malware on mobile device(smart phones) will evolve faster since techniques are already explored.

The early malware can only perform one or two tasks, like Cabir. Cabir was detected in 2004, it is the earliest mobile botnet we ever known.

But in 2009, the situation has changed dramatically. Mobile bots can connect back to a malicious bot server and transfer valuable information of the infected device, like SymbOS.Exy.C[6], Ikee.B[7,8]. According to the report of Symantec[6] on 13 July 2009, SymbOS.Exy.C may the first bot on Symbian OS. It is a worm similar to other worms that made for Symbian OS, but the difference is that the bot node tries to contact a malicious bot server and transfer valuable information, such as the phone types, International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI)[9]. Symantec mentions that this may be the first true botnet occurred on a cellular mobile device.

BBOS_ZITMO.B[10] was detected in 2011. It receives commands via SMS, steal users information by forwarding SMS messages to a set/predefined admin phone number, monitors incoming calls and SMS. The most important is that it also has a stealth mechanism that prevents being seen as an installed app.

Figure1 illustrates the simplified typical infection cycle of an SMS based mobile botnet. There are mainly 4 steps in the botnet operation [11]. Vulnerable smart phones could be first infected by bots in the original botnet. The existed techniques (smart phone OS vulnerabilities, Trojan horses, worms, etc) were used during the infection period. After the infection, the infected node connects to the bot server to join in the origin botner. All the bot servers are organized as the C&C network and controlled by bot master. Bot master use the C&C network to issue commands, and control the whole botnet. According to our analysis, the bots in the same tier or sub network could launch the corresponding attack after receiving the command. Authorization is achieved via a channel password.

doi:10.4304/jcp.7.1.235-243

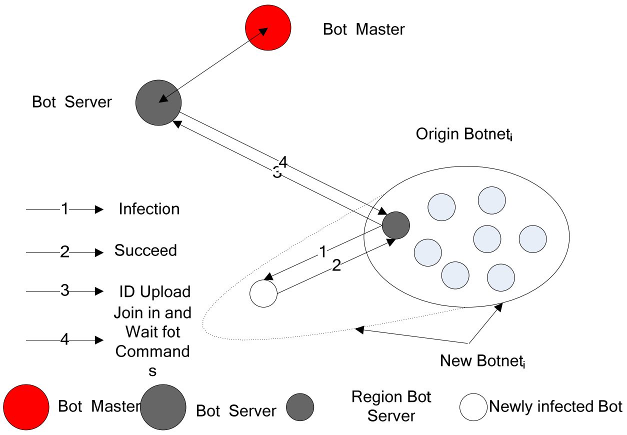


Figure 1 Typical infection cycle

Consider the potential threats of the mobile botnet to the cellular network. Researchers have done some remarkable research about the attacks on cellular network, such as DoS attack [12], C&C channel study[13], paging channel overloads [14].

In this paper, we proposed the SMS based heterogeneous mobile botnet. The C&C channel is SMS based heterogeneous multi-tree structured network. That is, all C&C commands are transfered via SMS messages since SMS is available to almost mobile phones. We use heterogeneous multi-tree topology to enhance the scalability and robustness of the botnet. We also made all the bot lists and some of the important commands encrypted.

Our research has the following main contributions:

- We proposed an improved SMS based heterogeneous mobile botnet. The heterogeneous bot nodes and networks structure have made the mobile botnet more efficient to communicate and more secure.
- Contrast with the traditional botnet of Internet world, we give the definition of mobile botnet and illustrate the characteristics of the mobile botnet.
- We introduced node degree threshold $\langle k \rangle$ and mobile botnet height H to improve the security of the C&C channel. The improved C&C channel raises the bar for the countermeasure of mobile botnet community.
- Through the design of the eviction and replacement mechanism of failed or recovered bot server node, the robustness of C&C channel was enhanced.

The remainder of the paper is organized as follows. Section II shows the characteristics of cellular bonnets. Section III illustrates the mobile botnet attacks. Section IV proposed our SMS based heterogeneous cellular mobile botnet. Section V discussed our model from the aspect of connectivity, security and robustness. The paper concludes and future work with Section VI.

II. THE CHARACTERISTICS OF MOBILE BOTNETS

In this paper we define the mobile botnet as follows:

Definition 1 mobile botnet: Consists of a network with compromised smart phones, controlled by attacker ("bot master") thorough a command and control("C&C") network for malicious purposes.

The mobile botnets are different from the traditional botnets of Internet world. Since the mobile botnets are mostly communicated between mobile devices (smart phones), it has the following characteristics.

- Limited by the power resource. The mobile devices such as smart phones are different from PC, its run time is limited due to the use of battery.
- The communication costs problems. The communications of mobile botnets will consume the limited power resource, network traffic and especially the phone charge. The communications of the mobile botnets will lead to the cost of the owner, and a significant rise of the phone charge will result in the investigation of the cause and thus may lead to the exposure of the culluar bot. The SMS based mobile botnets, depending on the type of mobile phone contract, SMS messages can be completely free or charging very few money.
- The connectivity changes constantly, even unstable. The connectivity may be both affected by physical environment or personal factors. It can be affected by the networks around the mobile phone owner, the action of the mobile phone owner, such as the user is in the tunnel or turn off the mobile phone during the bed time. As shown in Table 1, the connectivity of bots can be changed constantly during the daily life.

Table 1
THE CONNECTIVITY AND TIME INTERVAL

Connectivity	*Time Intervals*
WiFi	Morning (at home)
GSM/EDGE/3G	Day time (at work/school)
WiFi	Day time (at Starbucks)
No signal	Day time (at wild)
WiFi	Evening (at home)
Turn off the mobile phone	Night (bed time)

- Lack of IP address. The lack of IP address may cause the problem of indirect connect. Due to the lack of IP address, most mobile phones are using NAT gateway and thus the devices are not directly reachable, so the traditional P2P based C&C network may not suit for mobile botnet.
- The diversity of operating system of smart phone. The design of mobile botnet has to consider the diversity of the OS platform of smart phone.
- Mobile botnets are hard to be detected. Evidences indicate that, mobile botnets are becoming more and more sophisticated[10]. The valuable messages can be forwarded by SMS messages to a predefined server device, and the SMS messages are deleted immediately after they were forwarded by mobile botnets, so it is hard to be detected. It also has a stealth mechanism that prevents being detected as an installed app..

III. MOBILE BOTNET ATTACK

A. Information Leakage

One of the main targets of the mobile botnet is to retrieve sensitive information from the victims. The mobile bot can quickly scanning the host node for significant corporate or financial information, such as usernames and passwords, address list and text messages.

B. DoS Attack

Because most of the functionality of cellular network rely on the availability and proper functioning of HLRs(Home Location Register), so the DoS attack could block the legitimated users of a local cellular network from sending or receiving text messages and calls[9,12,15,17].

In the practical circumstances, a bot master of a mobile botnet could control the compromised mobile phones to overwhelm a specific HLR with a large volume of traffic. Through the DoS attack, it will affect all the legitimated users who rely on the same HLR, their requests will be dropped.

By overloading (red arrow) the HLR of a local central component of the cellular network, the network will unable to server legitimated traffic (blue arrow) of very large geographic regions. Figure 2 shows how a cellular network DoS attack occurs.

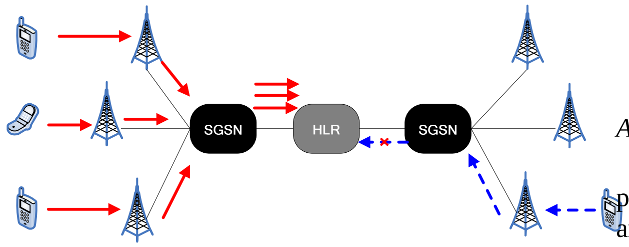


Figure 2 A cellular network DoS attack

C. Charge loss

There exist some service which the smart phones can give money to charity organizations[17]. If the mart phone called or sent a text message to the specific service number, then the subscriber will pays a preset amount of money. The bot master can also creates its own service number and programs all the bots to call or sent a text message to the specific service number. Of course, the price should be low, so the subscribers would not notice and be suspicious about the extra charges.

IV. SMS BASED HETEROGENEOUS MOBILE BOTNET DESIGN

As we known, the three main components of botnet are vectors, C&C channel and network topology. The vector solved the problem of how to spread bot code, and can be used in propagation period; C&C channel is used to issue command and control messages; the network topology of botnet is to manage the botnet and enhance the security and stealth of botnets.

Considering the problems that have been encountered during the design period of traditional botnets and mobile botnets, we think the bot master should consider the following challenges:

1. How to transmit command and control messages and control traffic flow.

2. How to prevent the proposed mobile botnet from being detected by defenders.

3. How to monitor the status of bot nodes.

4. How to enhance the robustness of mobile botnet even some bot nodes have been removed by the defenders.

In this section, we will propose the SMS based heterogeneous mobile botnet, and briefly overview our mobile botnet and all type of nodes and then focus on the propogation, network topology, command and control mechanism, node replacement mechanism of our mobile botnet. The designed mobile botnet model is shown in Figure 3.

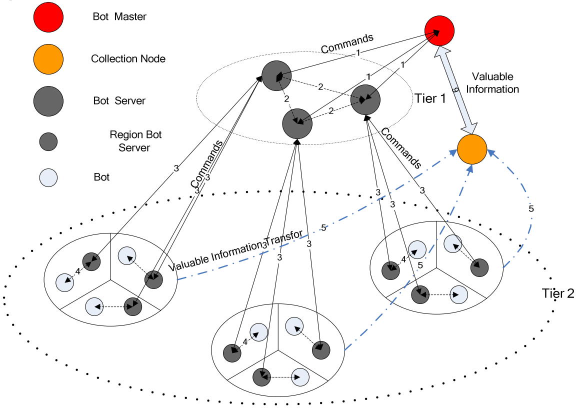


Figure 3 The simplified SMS-based heterogeneous mobile botnet

A. Node Types

The infected node can be classified by the difference of performance, battery resource, connectivity and networks around it, so they can be divided into several types of bot nodes. As is illustrated in Figure 3, our mobile botnet is made up of bot master, collection node, bot servers, region bot servers and a certain amount of bot nodes. The topology of our mobile botnet was designed multi-tree structured from top to down, but the topology of the same tier nodes such as bot server tier was designed P2P structured. So, the heterogeneous exist both in bot nodes types and network topology.

Bot master node: Bot master controls all the nodes of the mobile botnet. The bot master has direct contact with bot servers. It has the bot list of all the botnet, and it stores all the node's information, like user name, phone number, international mobile subscriber identity (IMSI), International Mobile Equipment Identity(IMEI). Unless an emergency situation, bot master will not communicate with bot node directly.

Collection node: It receives the valuable information from all the nodes of the botnet. The stored information can be fetched by bot master. Before it receives the information, the node that sends information must be authenticated.

Bot server node: Bot Server node is one of the key nodes of our model. It has two main functions, search and forward, it has $k^{'}$ direct links with region bot servers, and each of them controls a sub network. It has the bot list that includes all the nodes it communicated with, and the bot list is encrypted.

Region bot server node: Region bot server node is another key node of our model. It is both boy server and bot node. It receives commands from bot server and forwards to the bots of its sub network. It executes the commands and transfer valuable information to the collection node. Also its bot list was encrypted.

Bot node: Bot node is the leaf node of ourmobile botnet. It receives commands from region bot server, and executes the commands.

The comparison of communication and bot list between the five types of nodes that we have stated is shown in table2.

Table 2
THE COMMUNICATION OF MODEL NODES

Node type	Bot master		Collection node		Bot server		Region bot server		Bot	
	Commu.	Node list	Commu.	Node list	Commu.	Node list	Commu.	Node list	Commu.	Node list
Bot master		yes	yes	yes	yes	yes				
Collection node	yes	yes					yes	yes	yes	
Bot server	yes	yes			yes	yes	yes	yes		
Region bot server		yes	yes	yes	yes	yes			yes	
Bots		yes	yes	yes			yes	yes	yes	yes

B. Propogation

We divide the propagation phase into three steps.

In the first step, the bot master exploit the operating system and configuration vulnerabilities to compromise the mobile devices, install the bot software and collecting valuable information. After the bot software was installed, we assume the bot node has a stealth mechanism that prevents being seen as an installed app, and the messages that used to collect valuable information were deleted.

In the second step, the bot master choose bot server nodes from the compromised nodes as the first tier nodes according to the following conditions, the energy resource, the region where it belongs to and the connectivity. The rest of the nodes that are not chosen as the bot servers, assigned to the bot servers according the regions, as the second tier nodes.

The third step, the nodes of the existed botnets continued infecting mobile devices under the control of the bot master. According the expansion of the mobile botnet, the number of tier will grow.

C. Network Topology

Definition 2 Botnet degree: The degree of our mobile botnet is *K*. It is the maximum value of $\langle k_i \rangle, i \in N$.

Definition 3 Botnet height: The height of our mobile botnet is *H*. It is the number of tiers of the model.

Definition 4 A**tomic network:** The atomic network is composed of region bot node and $k^{'}$ bot nodes, it is the smallest bot network that was control by region bot server at the lowest tier.

Definition 5 $k^{'}$ **:** we define $k^{'}$ is the number of lower tier nodes that communicate with higher tier node n_i.

In general, our proposed mobile botnet is made up of 1 bot master, $k^{'}$ bot servers, $k^{'}$ region bot servers, and $k^{'}$ sub networks.

The maximum degree of bot server n_i is $\langle k \rangle = 2k^{'}$, in Figure 3, $k^{'}$ =3, $\langle k \rangle$ =6. For mobile botnets with large scale bot nodes, it makes sense to limit the degree of botnet *K* under a threshold. So, unless the bot nodes are high capacity server, bot masters should keep $\langle k \rangle$ small[14].

As we said, the topology of our model is heterogeneous multi-tree structured. From top to down, the model is a multi-tree structure network. The bot server tier and region bot server tiers are the P2P structured networks. The degree of the model is *K*, the height of the model is *H*. The degree of node n_i is $\langle k_i \rangle$, *K* is the maximum number of the degree of all the nodes, $K = \max(\langle k_1 \rangle, \langle k_2 \rangle, ..., \langle k_N \rangle)$. Our botnet(see Figure 3) can be divided into *H*-1 tiers and $k^{'}$ subnets. The lowest tier network contains $k^{'}$ ($k^{'}$ =3) subnet, and each subnet is composed of $k^{'}$ P2P structured atomic networks, as is shown in Figure 4.

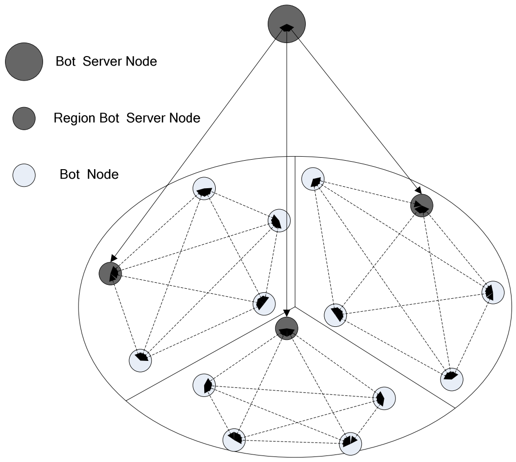


Figure 4 The simplified topology of the subnet of mobile botnet

The topology between bot server nodes is P2P structured network (tier 1in Figure 3), the distances between them are all 1 hop. Also the topology between region bot server nodes and bot nodes are P2P structured network. This will enhance the communication efficiency between the mentioned bot nodes,.

D. Command and Control Network

In our mobile botnet model, we use SMS as the C&C channel. Most of the traditional botnets are using centralized IRC, HTTP protocol and P2P based C&C channel, and all of these channels are IP-based C&C delivery. Unlike the PC world, even with the edge or 3G networks, the smart mobile devices (smart phones) still can not establish stable IP based connections with each other. Given this limitation, in our work we use SMS as our un-centralized and non-ip-based C&C channel.

The advantages of SMS based C&C channel can be listed as follows.

First, it is popular. Most of mobile phone subscribers are sending and receiving text messages to each other.

Second, it is easy to use. Malicious content can be hidden in message, the command and control messages can be disguised as spam-looking messages.

Third, it has high connectivity. Even a phone has signal problem or power off, the SMS messages that send to it will eventually arrive to it, because the SMS messages can be stored in a service center and delivered once the signal becomes available or turned back on[19].

Our mobile botnet can be considered as "PUSH" based botnet. The "PUSH" based botnet deliver commands form bot server to bot nodes whenever the bot master wants, and we call this process "PUSH". On the contrary, the traditional botnet [20] and [21] are the "PULL" based botnets, the bot nodes of them periodically communicate with bot server to get commands. But the "PULL" based botnets have some drawbacks, such as generate additional information, have unexpected latency in command delivery. G. Gu et al [18] has designed an effective detection schemes for it. All of the above statements made the "PULL" based botnets unattractive in practice. The "PUSH" based delivery does not generate additional information, and have little latency in command delivery, in this paper, we design our model as "PUSH" based botnet.

As is illustrated in Figure 3, The basic design idea for our SMS-based mobile botnet is to use a heterogeneous multi-tree network as the Command and Control(C&C) networks, the network is like a commands channel, all the nodes of network(black nodes) are served as bot server. The C&C network of our proposed model is composed of bot master, bot server and region bot server.

Like Kademlia[22], the absence of authentication mechanism means that anyone can insert values to the commands, the defender may use this launch index poisoning attacks and the C&C may be disrupted. So before communication the nodes should be authenticated, and the important command should be encrypted. For the efficiency of C&C, only critical commands issued by the bot master that order bots to execute malicious tasks such as "transmit valuable information" are encrypted, while commands for P2P communication purposes such as "search node" are only disguised without encryption[19].

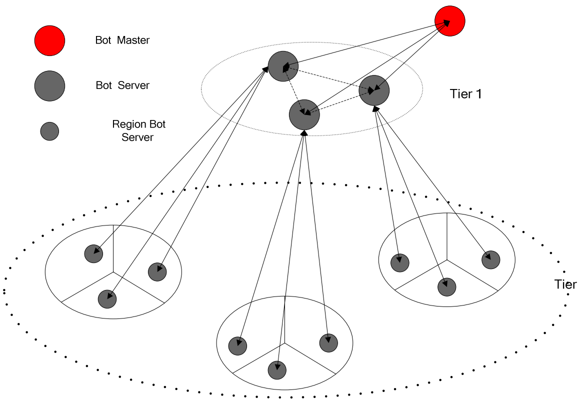


Figure 5 The C&C network

According to the bot list of it, bot server node performs two main function, search and forward. Some of the important commands are encrypted, and the encrypted commands are pushed from top tier nodes to lower tier nodes, from the bot master to bot server node, to region bot server node and bot node respectively. All of the bot lists are encrypted, once the key node was captured, the defender will not get the other nodes that communicate with it. And, also it cannot trace the bot master.

E . Node repalcement mechanism

At some special circumstances, bot node type may need to transfered from each other. Like one of the bot server node is failed or recovered.

The bot server nodes and region bot server nodes are the key nodes of our model, so they must be replaced by other nodes if they are out of function, such as failed or recovered. As is shown in Figure 6, at some circumstances, bot node type may need to transfer from each other. Since bot master has the bot list of the failed key node, by sending a message that containing the failed node's bot list and communication keys to the new key node and that will make it reconnected to the bots.

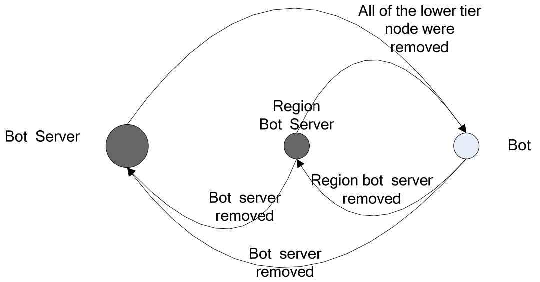


Figure 6 The transfer between three type of nodes

1) Node Eviction

Assumption1: we assume that the failed or recovered nodes can be detected by bot master.

Assumption2: we assume that all bot node have a self destroy mechanism to delete the bot list that stored in it.

Table 3
THE LIST OF NOTATIONS

Notation	Description
K_{BB}	Keys between bot server and bot master
K_{BS}	Keys between bot servers
K_{BR}	Keys between bot server and region bot server

First, the bot master detect the failed or recovered node n_i, then according to phone number of n_i that bot master stored in it to refresh the according keys, such as K_{BB}, K_{BS}, $K_{BR.}$ Second, the bot master sends $k'-1$ messages that contain the new keys K_{BS} to all the other bot servers, and send k' messages that contain K_{BR} to the region bot servers, which n_i communicate with. Third, the phone number of n_i was deleted from the bot list of bot master, bot server and region bot server.

After the eviction period, the failed or recovered node n_i can not communicate with the bot nodes that we have mentioned, and also the messages that send to them were discarded automatically. The eviction procedure is illustrated in Figure 7.

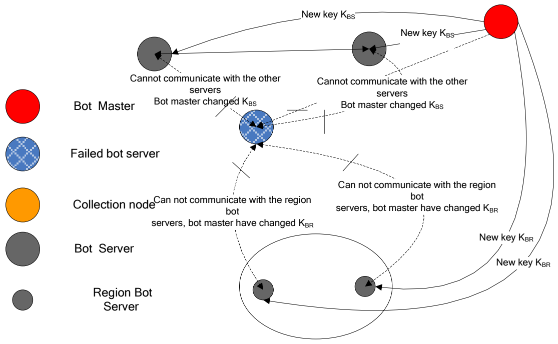

New key K_{BS}
New key K_{BS}
Cannot communicate with the other servers
Bot master changed K_{BS}
Cannot communicate with the other servers
Bot master changed K_{BS}
Bot Master
Failed bot server
Collection node
Bot Server
Region Bot Server
Can not communicate with the region bot servers, bot master have changed K_{BR}
Can not communicate with the region bot servers, bot master have changed K_{BR}
New key K_{BR}
New key K_{BR}

Figure 7 The eviction of failed or recovered bot server node

2) Node Replacement

At the replacement period, first, bot master choose a relatively powerful node from low tier bot nodes or region bot server as the new bot server according to standers that we have stated in *propagation* section. Second, the bot master send 1 message that contains the new keys K_{BB}, K_{BS}, K_{BR} and bot list to the new assigned bot server. Third, the new bot serner need to send $k'-1$ messages to establish communication with the rest bot servers and k' messages to establish communication with the region bot servers that were communicated with the captured bot server, so the total number of messages during the replacement period is $2k'-1$. The replace procedure is illustrated in Figure8.

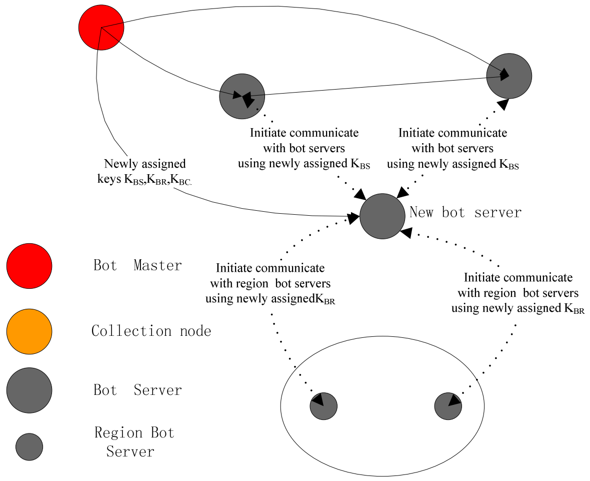

Newly assigned keys K_{BS},K_{BR},$K_{BC.}$
Initiate communicate with bot servers using newly assigned K_{BS}
Initiate communicate with bot servers using newly assigned K_{BS}
New bot server
Bot Master
Collection node
Bot Server
Region Bot Server
Initiate communicate with region bot servers using newly assignedK_{BR}
Initiate communicate with region bot servers using newly assigned K_{BR}

Figure 8 The replacement of bot server node

V. EVALUATION

In this section, we would like to analyze our proposed mobile botnet from the aspect of connectivity, security, and robustness.

A. Connectivity

In this section, we will discuss the connectivity of our heterogeneous botnet with different scale of node, and compare the connectivity with the P2P structured botnet.

We will look at the 200-node botnet first and then the 1000-node and 2000-node botnet. In the 200-node botnet, when k'=4 and k'=5, all the nodes in the botnet can be reached in 4 hops, and when k'=3, all the nodes in the botnet can be reached in 5 hops, as is shown in Figure 8. In the 1000-node botnet, as is illustrated in Figure 9, all the nodes can be reached in 5 hops when k'=4 and k'=5, and when k'=3, all the nodes can be reached in 6 hops. Figure 10 shows the 2000-node botnet, all the nodes will be reached in 5, 6, 7 hops respectively.

From Figure 9, 10, 11, we can see that the larger of k', the less hops mobile botnet needs to reache all the bot node of it, when the number of hops larger than 3, the connectivity will rise dramatically.

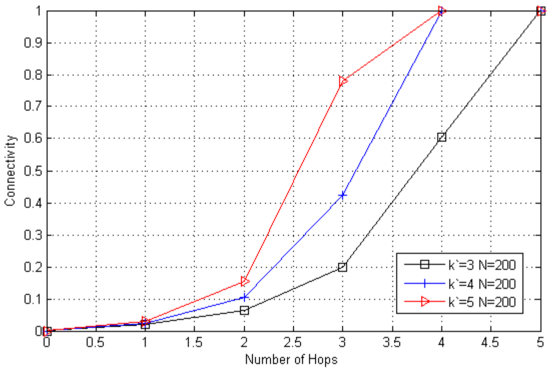


Figure 9 The relationship between connectivity and k', when N=200

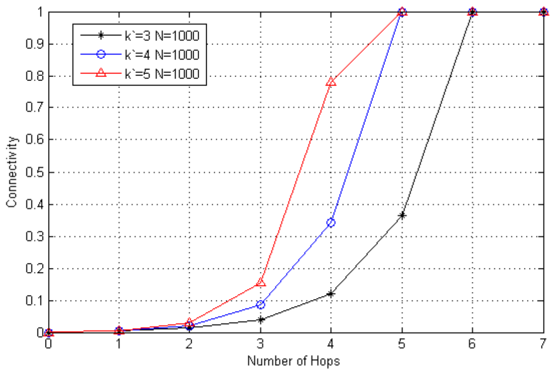


Figure 10 The relationship between connectivity and k', when N=1000

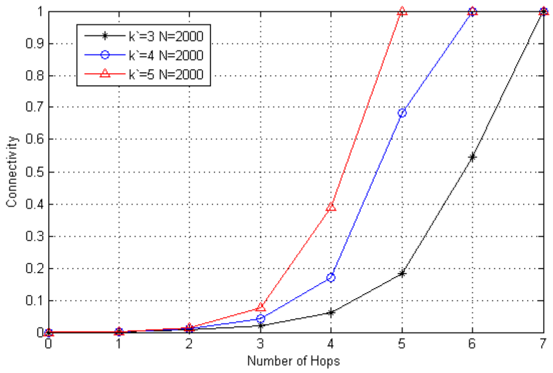
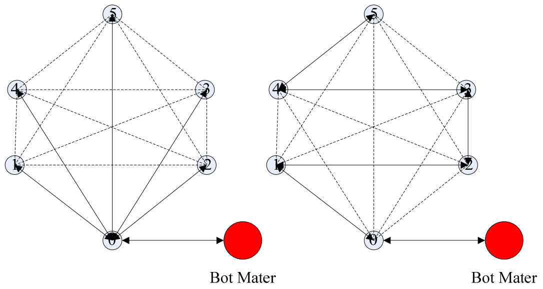


Figure 11 The relationship between connectivity and k', when N=2000

We compare our proposed botnet with the P2P structured botnet. In the P2P structured botnet, the average path length between any two nodes can be 1 hop to N hops.



(a)The shortest path length (b)The longest path length

Figure 12 the path length of P2P structured Botnet

As is illustrated in Figure 11(a), in the P2P structured botnet, the commands from *Bot$_0$* can be directly forward to *Bot$_1$*, *Bot$_2$*, *Bot$_3$*, *Bot$_4$*, *Bot$_5$*. So the mean path length is

$$PL_{P2P\,structured\_1} = \frac{\sum_{i=1}^{N-1} l_i}{N-1} = \frac{\sum_{i=1}^{N-1} 1}{N-1} = 1 \qquad (1)$$

In Figure 8(b), the commands from *Bot$_0$* can finally forward to *Bot$_5$*, through *Bot$_1$*, *Bot$_2$*, *Bot$_3$* and *Bot$_4$*. So the mean path length is

$$PL_{P2P\,structured\_2} = \frac{\sum_{i=1}^{N-1} l_i}{N-1} = \frac{\sum_{i=1}^{N-1} i}{N-1} = \frac{N}{2} \qquad (2)$$

According to Formula (1) and (2), the mean path length of the P2P structured botnet is

$$Mean_{P2P\,structured} = \frac{1+\frac{N}{2}}{2} = \frac{2+N}{4} \qquad (3)$$

So the mean connection hops between two nodes of the P2P structured botnet is $\frac{2+N}{4}$. When N =6, the mean connection hops is 2, it has nice network connectivity, but when N=200 and 2000, the mean connection hops are approximately 50 and 500, respectively, and it larger than our proposed botnet.

From the comparison, we can see that our proposed mobile botnet have high connectivity and it can be adjusted easily by adjust the height and scale of mobile botnet. It has high flexibility and scalability.

B. Security

As we described in section IV, the height of the model is *H*, $k^{'}$ is the number of lower tier nodes that communicate with heighter tier node. As is illustrated in Figure 5, the maximum number of nodes at the lowest tier is $(k^{'})^{H}$. Then, the maximum number of our proposed botnet model is

$$N = \sum_{i=0}^{H-2} (k^{'})^{i} + (k^{'})^{H} \qquad (1)$$

The larger of the *H*, the less community load of the key node. But large *H* will lead to long cummunication path and low connectivity. The relationship between model degree *K* and node degree $\langle k_i \rangle$ is

$$K = \max(\langle k_1 \rangle, \langle k_2 \rangle, ..., \langle k_N \rangle) \qquad (2)$$

$$\langle k \rangle \le 2k^{'} \qquad (3)$$

As we can see form Formula (2) and (3), *K* increase with the increase of $k^{'}$. During the C&C period, the key nodes have to forward at least $k^{'}$ messages at one time, but the large $k^{'}$ means that there is large scale of abnormal data traffic, and that will jeopardize the safety of key nodes. The relationships of $k^{'}$, *N*, and *H* are shown in Figure 9. When $k^{'}$ =3 and the value of *H* are 2, 3, 4, 5 respectively, the proposed botnet will have better connectivity but have lower capacity. When the value of $k^{'}$ is 5, there is a better leverage between connectivity and N. In this paper, consider the tradeoff between $k^{'}$ and N, we set our mobile botnet *H*=5, $k^{'} \le 5$, so $\langle k \rangle \le 10$, $K \le 10$, and the scale of the botnet can up to 3281 bot nodes.

By the tradeoff between k' and H, we can efficiently control the amount of traffic flow that travels between bot nodes, and the communications between bot nodes will not catch the attention of defender and then protect the mobile botnet, so our mobile botnet can have high security.

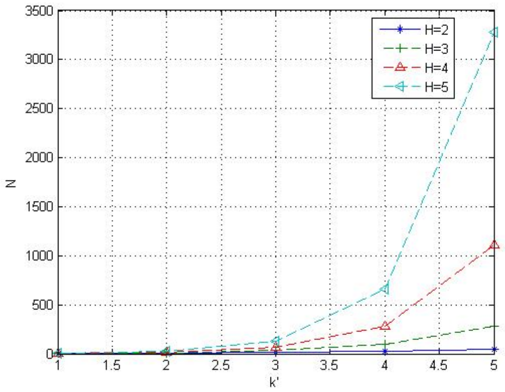


Figure 13 The relationship of *k'*, *N* and *H*

C. Robustness

As we discussed in section II, Battery consumption plays a very important role in the cellular world. So it is a challenge for the mobile bot not to drain the battery significantly, otherwise, it will jeopardize the security of the bot nodes. High CPU load and heavy forward usage are the main causes of the battery drain of bot node.

Based on our study, radio usage cost more energy, so we are more concerned about the forward usage. Hence our mobile botnet has "PUSH" based delivery mechanism, the commands from the bot master are direct transferred by bot servers to bot nodes, and no additional messages are generated.

Before C&C channel repair, the bot master need to check if the communication multi-tree has broken at some key nodes, all it has to do is broadcast ping and every node need to answer it. Obviously, the check of the communication multi-tree is important, and need to perform periodically. The check may also perform at some sub networks at one time so that it will not cause the attention of the defender.

As is shown in Figure 14, if the height of botnet is 5, the maximum degree of 200-botnet is 3, the maximum degree of 200-botnet is 5, the eviction needed messages of 200-botnet are 5, and the eviction needed messages of 2000-botnet are 9. As we have seen that the number of eviction needed messages are acceptable and the eviction of recovered bot node of our botnet is feasible and can save the limited energy resource.

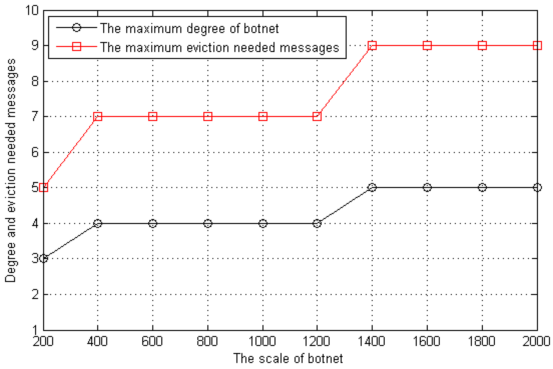


Figure 14 The relationship between the degree of botnet and eviction needed messages

We set the height of botnet is 5, the maximum degree of 200-botnet is 3, the maximum degree of 200-botnet is 5, the replacement needed messages of 200-botnet are 6, and the replacement needed messages of 2000-botnet are 10. Also, from Figure 15, we can see that the replacement of our botnode is easy and energy resource saved.

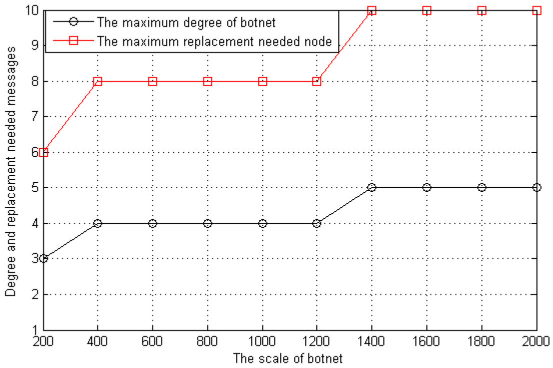


Figure 15 The relationship between the degree of botnet and replacement needed messages

The eviction and replacement period has strong operability, and the messages that needed of our botnet is acceptable, so we can say that our botnet has strong robustness.

VI. Conclusion

In this paper, we proposed the SMS based heterogeneous mobile botnet. The heterogeneous bot nodes and networks structure have made the C&C channel more efficient and secure. The communication protocol, botnet height and degree control mechanism, the node replacement of our mobile botnet is reasonable and acceptable. From the evaluation section, we can see that our mobile botnet has a highly connectivity, security and robustness.

Our future work includes the intensive study of C&C protocol of botnets, such as SMS-based C&C protocol and IP-based C&C protocol. We plan to study the authentication algorithm and encryption algorithm of bot node communications of our mobile botnet. Meanwhile, we would like to study the counter measures of SMS based mobile botnets.

Acknowledgment

The work described in this paper has been supported by Major Program of National Science and Technology (2011ZX03002-005-01), Key Project of Chinese Ministry of Education and National Key Technology R&D Program (2009BAH39B02), China Postdoctoral Science Foundation funded project (20100471762).

References

[1] Geer D, "Malicious bots threaten network security," IEEE Computer, 2005,38(1):18-20.

[2] LiPeng Song, Jin Zhen, GuiQuan Sun, "Modeling and analyzing of botnet interactions," Physica A 390 (2011) 347–358.

[3] LiPeng Song, Jin Zhen, GuiQuan Sun. "Influence of removable devices on computer worms: Dynamic analysis

and control strategies," Computers and Mathematics with Applications 61 (2011) 1823–1829

[4] Lee WK, Wang C, Dagon D," Botnet Detection: Countering the Largest Security Threat," New York: Springer-Verlag, 2007.

[5] Norman ASA. Mobile phone threats - hype or (finally) truth? Security Articles -Archive, 2009. http://www.norman.com/security_center/security_center_archive/2009/67174/en, read: 2009.05.31.

[6] Irfan Asrar. Could sexy space be the birth of the sms botnet? Symantec, Internet blog, jul 2009. http://www.symantec.com/connect/blogs/ could-sexy-space-be-birth-sms-botnet, read: 2009.07.30.

[7] Ikee.B, http://www.symantec.com/security response /writeup.jsp?docid=2009-112217-4458-99.

[8] P.A. Porras, H. Saidi, V. Yegneswaran, "An Analysis of the iKee.B iPhone Botnet," in Proceedings of the 2nd International ICST Conference on Security and Privacy on Mobile Information and Communications Systems (Mobisec), May 2010

[9] A. Mehrotra and L.S. Golding. Mobility and security management in the gsm system and some proposed future improvements. Proceedings of the IEEE, 86(7):1480-1497, Jul 1998.

[10] BBOS_ZITMO.B http://about-threats.trendmicro.com/ Malware.aspx?language=us&name=BBOS_ZITMO.B

[11] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis. A multifaceted approach to understanding the botnet phenomenon. In Internet Measurement Conference, 2006.

[12] 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 Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'09)

[13] K. Singh, S. Sangal, N. Jain, P. Traynor, and W. Lee, "Evaluating bluetooth as a medium for botnet command and control," in Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2010).

[14] J. Serror, H. Zang, and J. C. Bolot. Impact of paging channel overloads or attacks on a cellular network. In Proceedings of the ACM Workshop on Wireless Security (WiSe), 2006.

[15] Anne Ruste Flø, Audun Jøsang. "Consequences of Botnets Spreading to Mobile Devices," short-paper Proceedings of the 14th Nodic Conference on Secure IT System (NordSec 2009).

[16] David Dagon, Guofei Gu, Cliff Zou, Julian Grizzard, Sanjeev Dwivedi, "A Taxonomy of Botnets," University of Central Florida, 2005.

[17] Anne Ruste Flø, Audun Jøsang. "Consequences of Botnets Spreading to Mobile Devices," short-paper Proceedings of the 14th Nodic Conference on Secure IT System (NordSec 2009).

[18] G. Gu, R. Perdisci, J. Zhang, and W. Lee. Botminer: Clustering analysis of network traffic for protocol- and structure- independent botnet detection. In Security, 2008.

[19] Yuanyuan Zeng, Xin Hu, Kang G. Shin, "Design of SMS Commanded-and-Controlled and P2P-Structured Mobile Botnet", The University of Michigan, Ann Arbor, MI 48109-2121, U.S.A. 2009.

[20] P. Wang, S. Sparks, and C. C. Zou. An advanced hybrid peer-to-peer botnet. In USENIX Workshop on Hot Topics in Understanding Botnets (HotBots'07), 2007.

[21] R. Vogt and J. Aycock. Attack of the 50 foot botnet. Technical report, 2006.

[22] P.Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric," in IPTPS, 2002.

Guining Geng, male, was born in 1981. He received his Bachelor Degree in college of computer science and technology from QUFU Normal University in 2006, and received his Master Degree in college of computer science and technology from Harbin Engineering University in 2009. He is now a Ph.D Candidate in Beijing University of Posts and Telecommunications. His research interests are cryptography and Mobile Internet Security.

Guoai Xu, male, was born in1972. He received the Ph.D degree from School of Information Engineering, Beijing University of Posts and Telecommunications, Beijng, China, in 2001. He is now a professor in BUPT. His research interests include Information Security Management, Software security and so on.

Zhang Miao, male, was born in March, 1980. He received the Ph.D degree from School of Information Engineering, Beijing University of Posts and Telecommunications, Beijng, China, in 2007. He is now a teacher in BUPT. His research interests include Software security, Mobile internet and so on.

Yanhui Guo is a an associate professor in Beijing University of Posts and Telecommunications. She received her Ph. D. in Signal and Information Processing from Beijing University of Posts and Telecommunications in 2003. Dr.Guo was also a visiting scholar in the School of Information Sciences in the University of Pittsburgh in 2009. She has published a number of papers in international conferences and journals. She is interested in intelligent information processing and information content security.

Guang Yang, female, was born in 1980. She received his Bachelor Degree in college of computer science and technology from Heilongjiang University in 2003, received her Master Degree and Doctor Degree in college of computer science and technology from Harbin Engineering University in 2007 and 2009, respectively. Her research interests are Mobile Internet Security and WSN Security.

Cui Wei is an engineer in Information Center of Ministry of Science and Technology of the People's Republic of China. He received his Ph. D. in cryptography from Beijing University of Posts and Telecommunications in 2009. Cui wei has published a number of papers in international conferences and journals. He is interested in signature and information security.