Chord-based Quantum Botnet Research

Wang Xin-Liang*[1], Lu Nan[2], Gao Qing-Hua[3]
[1]School of Electrical Engineering and Automation, Henan Polytechnic University,
[2]The Research Institution of China Mobile,
[3]School of Electrical Engineering and Automation, Henan Polytechnic University,
*Corresponding author, e-mail: junci158@163.com[1], lunan@chinamobile.com[2], gaoqh@hpu.edu.cn[3]

Abstract

In order to make the controller better to master the botnet, the traditional chord-based botnets ensure that all adjacent nodes can maintain the periodic communication so that the routing table of every node could keep accurate and efficient. The periodic communication behavior will also increase the risk of exposure of the traditional chord-based botnets. Once one of the peers is captured by network security device, more peers will be captured based on periodic communication behavior of chord-based botnets that leads to affect the botnet robustness. For the aforementioned problems in the traditional chord-based botnet, this paper will construct a quantum botnet control platform based on the improved B92 protocol. The in-depth analysis showed that the infected hosts in the chord-based quantum botnet can more quickly be increased, and can maintain a larger scale compared with the traditional chord-based botnet. So the chord-based quantum botnet owns better robustness and stability.

Keywords*: chord, quantum botnets, periodic communication, quantum communication*

1. Introduction

Botnet [1] is a victim’s computer group controlled by the attacker through the control server, and poses a great threat on network security, national security. In traditional IRC-based botnets, the whole network is controlled by an IRC server. Once IRC server is exposed in the process of information transfer, it will lead to the destruction of the entire botnet; the hardware and software resources of IRC server are limited that limits the effective scale(<5000) of the IRC-based botnets [2]. New P2P-based botnets own a strong ability to survive, and own the distributed characteristics that make it a strong resistance to detecting of security devices. When some node in p2p-based botnet is found, it will not expose the entire network to protect the network security to a certain extent; the distributed structure improves the operation efficiency of the entire network, in order to ensure that the message delay is in a reasonable range. It will make the attacker easier to launch DDOS when needing to coordinate the participation of a large number of hosts at the same time. Meanwhile, the structured P2P-based botnets have good scalability and self-organization ability. In the p2p-based botnets, the chord-based botnet is a fully structured one that has distributed architecture, scalability, high communication efficiency.

In order to make the controller better to master the botnet, the chord-based botnets ensure that all adjacent nodes can maintain the periodic communication [3] so that the routing table of every node could keep accurate and efficient. The periodic communication behavior will also increase the risk of exposure of the chord-based botnets. Once one of the peers is captured by network security device, more peers will be captured based on periodic communication behavior of chord-based botnets that leads to affect the botnet robustness [4-8]. To solve the above problem, if the quantum secure communication can be used to realize the update of the routing table instead of the classical communication, it will pose a greater impact on increasing the security of chord-based botnets.

BB84 [9] was proposed as the first quantum key distribution protocol by Bennett and Brassard in 1984. In 1991, Ekert proposed a new type of quantum key distribution protocol E91 [10] by EPR entangled particles that relies on Bell inequality to ensure the security of key distribution. In 1992, Bennett proposed a more simple quantum key distribution protocol, referred as B92 [11] that any two non-orthogonal states can be used to implement the key

Received November 8, 2013; Revised June 28, 2014; Accepted July 25, 2014

distribution [11]. In 1995, L.Goldenberg and L.vaidman proposed a key distribution protocol based on orthogonal quantum states [12]. Meanwhile, the other key distribution protocols have successively been proposed so that the keys could be more efficient to distribute. In recent years, quantum secure direct communication (QSDC) protocol [13-17] has been proposed as a new type of quantum cryptography communication protocol. The QKD and QSDC need to use the classical channel to publish part of the information that is used to detect the presence of eavesdropping and ensure the safety of the channel. So, if the above protocols are directly used to achieve the periodic communication in chord-based botnet, network security devices can track the classical channel to achieve the detection of periodic behavior, resulting in the deterioration of safety performance in the chord-based quantum botnet.

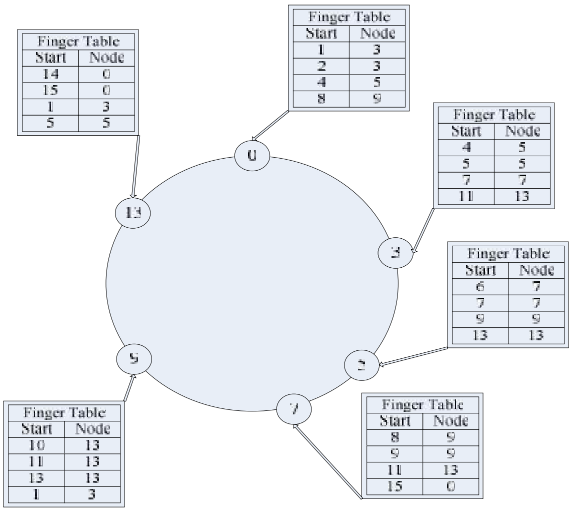
To solve this problem, this paper will construct a control platform that botnets can effectively detect the existence of eavesdropping in the process of periodic communication process by using the improved B92 protocol. The improved B92 protocol does not need to use the classic channels in the process of periodic communication, so it can not only detect the eavesdropping in the quantum channels, but also avoid the tracking of network security devices in the classical channels. In total, the chord-based quantum botnet can improve the safety performance and control efficiency of the botnet, and provide a theoretical basis for research and defense of the quantum botnets.

2. Traditional Chord-based Botnet

Chord is a structured p2p network that is fully de-centralized and distributed, and the network topology of chord-based botnet is shown in Figure 1. It uses a variant of consisitent hasing to allocate an m bit identifier for each node in chord-based botnet, and the node identifier can be generated by hashing the ip address of node. The ring size is determined by the m that ranges from 0 to 2^m-1, and the nodes are arranged in a clockwise. If m is 160, the chord-based botnet can accommodate up to 2^{160} nodes that is a very large scale. Each existing node in the ring can have the functions similar to the super-node, and can publish control commands. It embodies a completely decentralized characteristic that any one peerbot is equally important to ensure the robustness of chord-based botnet.

Each node in the chord-based botnet maintains part of the routing table, called the finger table. There are $\log_2 n$ entries in the finger table, and the ith entry stores the successor of node that its length is $N + 2^{i-1}$. When the attacker releases the control commands through some node, the node will transmit the commands to other nodes in the own routing table by broadcasting. Meanwhile, the other nodes will also transmit the above commands to the nodes in their own routing tables, so until every node receives the control commands. As shown in the Figure 1, m = 4, that is to say, there are up to 16 nodes in the logical ring. Assuming that the actual nodes in the chord-based botnet are 0, 3, 5, 7, 9, 13, the attacker can arbitrarily choose the node to release control commands [3, 18]. First of all, some node will be determined as the publisher for issuing the control commands. Secondly, the first node as the publisher needs to release the control commands to the other nodes in its own routing table. Meanwhile, in order to avoid that a node repeats to receive the same control commands, the nodes will be assigned a relative limiting interval. Assuming that the ith entry in the routing table of some node points to the node j, its restriction point is the node $j^{'}$ that the i+1 th entry points to. Thus, when the node j receives control commands, it will send the commands to the other nodes in its routing table, but it is also subject to limitations, the node identifiers are between j and $j^{'}$. This ensures that a node in the ring will not repeat to receive the control commands, and the efficiency can be improved. The mechanism of information distribution in chord-based botnet can make the control more convenient, and at the same time, because each node only broadcasts to a limited number of nodes in the routing table, it will not cause much change of the network traffic. Compared to the flooding mechanism, botnet owns a higher security.

In the chord-based botnet, it is a import problem how to ensure that the routing table is correct. To solve the above problem, each node periodically needs to determine whether the entries of routing table are correct. If not correct, some changes will be made. It depends on the periodical interval for updating the routing table that the degree of accuracy and efficiency in the routing table can be improved. When the node exits due to some non-anti-reason, the ring will be broken. Assuming that the node n between n_p and n_s non-normally exits, the node n_p will periodically update the information of routing table. Firstly, n_p will try to ask n that has left the botnet, and when n_p does not receive a reply of the node n, it might try for a few times. If not received after a certain time, it is judged that the node n has left the network. At this time, n_p will find the next node in the routing table as a successor so that the routing table could be timely and accurately updated



Finger Table	
Start	Node
14	0
15	0
1	3
5	5

Finger Table	
Start	Node
1	3
2	3
4	5
8	9

Finger Table	
Start	Node
4	5
5	5
7	7
11	13

Finger Table	
Start	Node
6	7
7	7
9	9
13	13

Finger Table	
Start	Node
10	13
11	13
13	13
1	3

Finger Table	
Start	Node
8	9
9	9
11	13
15	0

Figure 1. Network Topology of Chord-based Botnet

3. Chord-based Quantum Botnet

The chord-based quantum botnet is proposed to realize the update of routing table in the peerbot and to avoid the tracking of security devices. It constructs the quantum secure channel between the peerbot and its adjacent nodes by using the uncertainty principle of quantum, as shown in Figure 2. If the B92 protocol is directly used for the update of routing table, the botnet needs to compare the measurement results by the classical channel in order to determine whether there exists eavesdropping in the quantum channel. However, the update of routing table is a periodic communication behavior, if each update always uses the classical channel to transfer data, the security devices can achieve the tracking and detection of botnet by monitoring the periodic update.

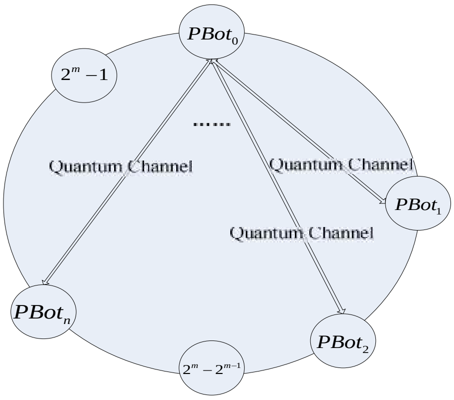


Figure 2. Network Topology of Chord-based Quantum Botnet

Therefore, B92 can't directly be used for the periodic update of routing table, and it needs to be improved based on the periodic characteristics in the chord-based quantum botnet. The improved B92 protocol works as follows:

Assume that the node that needs to update the routing table is denoted by $PBot_0$, and its adjacent nodes are denoted by $PBot_1$ $PBot_2$ … $PBot_n$. Network topology of chord-based quantum botnets is shown in Figure 2, and the specific updating process is as follows:

1) The chord-based quantum botnet will try to infect as many zombie hosts by the spam, remote intrusion, and so on. After the destination host is infected, the relative malware that owns the key K_{PBi} will be implanted in the infected host, so that it could achieve the encrypted communication with the other peer bots. The other peers own the communicate key K_{PBi}, and the symmetric encryption system is used in this paper.

2) Assuming that the infected host is denoted by $PBot_0$, when $PBot_0$ joins the chord-based quantum botnet, it needs to construct the own routing table by connecting some peer. In this stage, the information will be encrypted and decrypted by the key K_{PBi} in order to ensure the information security of botnet. Meanwhile, the random authentication key K_{PBAi} will be assigned between $PBot_0$ and its i-th adjacent peer for the periodic communication. The key length is $n^{'}$ bit. After information exchange is completed, the classical channel will be turned off.

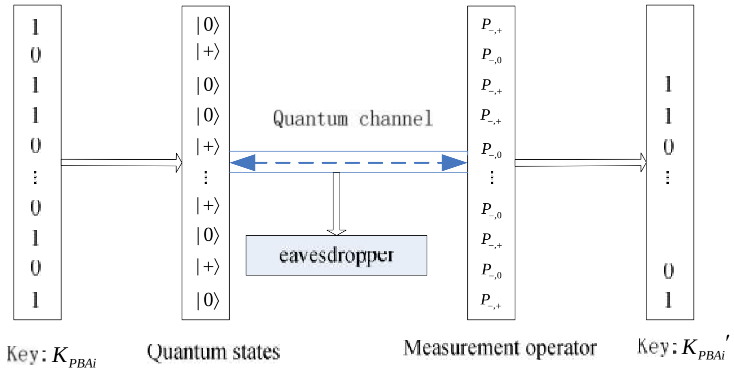


Figure 3. Periodic Communication Quantum Channel Based on the Improved B92

3) $PBot_0$ sends the authentication key K_{PBAi} according to a fiexed or non-fixed time interval so that it can determine whether its i-th adjacent peers is still online. The periodic communication module in quantum channel is shown in Figure 3, and the specific process is as follows:

a) $PBot_0$ prepares n qubits, and the encoding rule is shown in Table 1. $|0\rangle$ and $|+\rangle$ are two non-orthogonal quantum states that are normalized, and $0<\langle 0|+\rangle<1$. $P_{-,0}=1-|0\rangle\langle 0|$, and $P_{-,+}=1-|+\rangle\langle +|$. $P_{-,0}$ and $P_{-,+}$ are respectively projected onto orthogonal states of $|0\rangle$ and $|+\rangle$. That is to say, $P_{-,0}|0\rangle=(1-|0\rangle\langle 0|)|0\rangle=0$, $P_{-,0}|+\rangle=(1-|0\rangle\langle 0|)|+\rangle=|+\rangle-|0\rangle\langle 0|+\rangle$, $P_{-,+}|+\rangle=(1-|+\rangle\langle +|)|+\rangle=0$, $P_{-,+}|0\rangle=(1-|+\rangle\langle +|)|0\rangle=|0\rangle-|+\rangle\langle +|0\rangle$. When the measurement result is not 0, the state of the quantum bit can be determined according to the above equation.

Table 1. Encoding Rule

No.	Polarization state	Classic bits	Measurement Operator
1	$\vert +\rangle$	0	$P_{-,0}$
2	$\vert 0\rangle$	1	$P_{-,+}$

b) $PBot_0$ sends the prepared quantum bit one by one through the quantum channel to the i-th adjacent peer. Assuming that the quantum bits that some adjacent peer receives are denoted by q, and the j-th quantum bit is denoted by q_j, for all adjacent peers has pre-stored authentication key K_{PBAi}, the appropriate measurement operator will be selected according to K_{PBAi}. Assuming that the j-th bit of K_{PBAi} is denoted by p_j, if $p_j = 0$, the operator $P_{-,0}$ will be used to measure; if $p_j = 1$, the operator $P_{-,+}$ will be used to measure. Although the selection of measurement operator is completely correct, for its encoding rule is based on the non-orthogonal quantum states, it is still possible that the quantum bit can not be correctly recovered. Assuming that $\vert 0\rangle = \vert\rightarrow\rangle$ and $\vert +\rangle = \vert \quad \rangle$, the probability are 50% that the quantum state can not be correctly recovered, the specific process is shown in Figure 3.

c) The i-th adjacent peer will compare all the detected quantum bits with the quantum bits in same position of K_{PBAi}. If no noise in the quantum channel, both sides will be consistent; if inconsistent, there exists the eavesdropper in the quantum channel. On the contrary, the bit error rate will be produced. Assuming that the upper limit of bit error rate is set to R', if the bit error rate measured $R > R'$, there exists eavesdropping in the quantum channel. When detecting the eavesdropper, $PBot_0$ and the i-th adjacent peer will automatically terminate the periodic communication to ensure the security of entire network.

d) After the i-th adjacent peer correctly receive the key, it will send K_{PBAi} to $PBot_0$ in the same manner to make $PBot_0$ update its routing table.

In the chord-based quantum botnet, it can effectively monitor the existence of the eavesdropping, so it becomes impossible that the security device detects the botnet based on time pattern of periodic communication, and the safety of entire botnet will eventually be guaranteed.

4. Performance Analysis

In the chord-based botnet, the infected peers will spread the virus to infect more hosts as much as possible, and some peers will be removed when they are discovered by the security devices. In this paper, SIR model will be used to describe the entire process of botnet operation. In this model, the largest number of hosts in the chord-based botnet is denoted by $N(t)$ at time t, the number of infective hosts at time t is denoted by $I(t)$, the number of susceptible hosts is denoted by $S(t)$, the number of recovered hosts at time t is denoted by $R(t)$, the infection rate in the period is denoted by , the immune rate in the period is denoted by ¥ , and ∂ is the number of infected peers that the security devices can capture by tracking some infected host based on the periodic update of routing table.

In the traditional chord-based botnet, for it uses the classical channel to complete the update of routing table, the security device can capture more infected peers by tracking the periodic traffic that some infected host produces, and the entire botnet can be described by the following equations:

$$\frac{dI(t)}{dt} = \quad S(t)I(t) - ¥I(t) - \partial ¥ I(t)$$
$$\frac{dS(t)}{dt} = - \quad S(t)I(t)$$
$$\frac{dR(t)}{dt} = ¥I(t) + \partial ¥ I(t)$$
$$N(t) = I(t) + S(t) + R(t)$$

In the chord-based quantum botnet, for it uses the entire quantum channel to complete the update of routing table, the security device can't capture more infected peers by tracking some infected host, and the entire botnet can be described by the following equations:

$$\frac{dI(t)}{dt} = \quad S(t)I(t) - ¥I(t)$$
$$\frac{dS(t)}{dt} = - \quad S(t)I(t)$$
$$\frac{dR(t)}{dt} = ¥I(t)$$
$$N(t) = I(t) + S(t) + R(t)$$

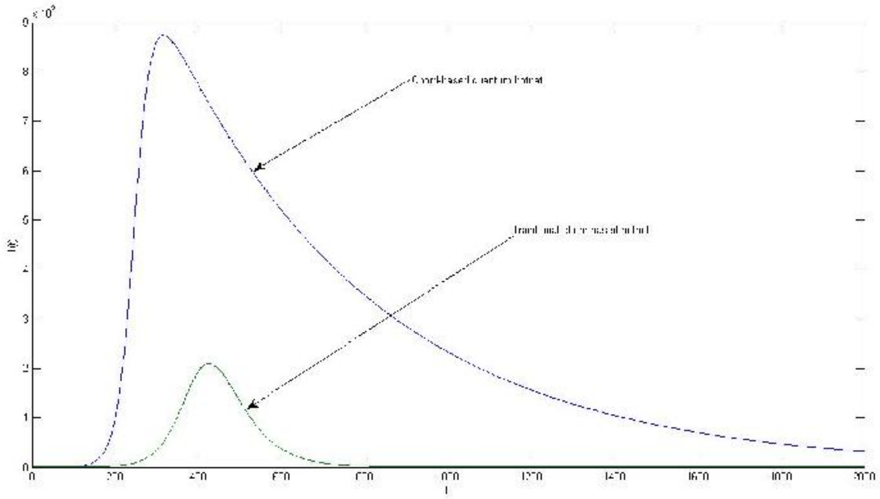


Figure 4. I(t)

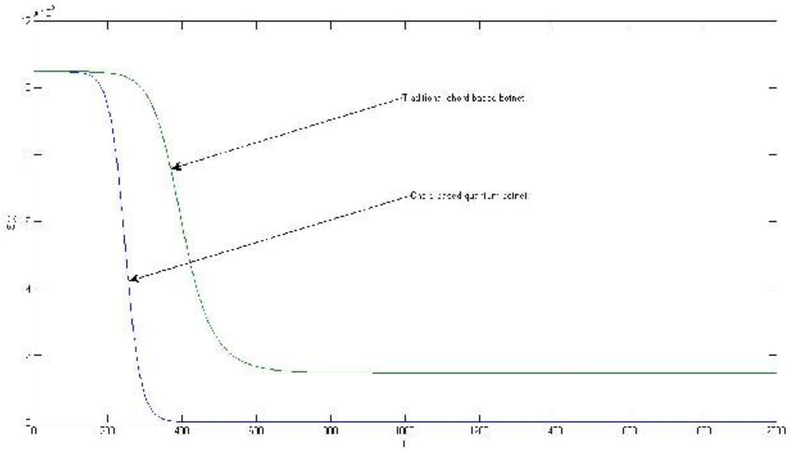


Figure 5. S(t)

Assuming that $N(t) = 2^m$, $m = 20$, $I(0) = 10$, $S(0) = 2^{20} - I(0) = 2^{20} - 10$, $= 0.05 / N(t)$, ¥ $= 0.002$, $\partial = m/2 = 10$, $I(t)$ and $S(t)$ in the chord-based botnet are individually shown in Figure 4, 5. With reference to Figure 4 the infected hosts $I(t)$ in the chord-based quantum botnet can more quickly be increased, and can maintain a larger scale compared with the traditional chord-based botnet. With reference to Figure 5 $S(t)$ in the chord-based quantum botnet decreases more quickly compared with the traditional chord-based botnet, that is to say, the chord-based quantum botnet can infect more hosts to magnify the scale of botnet. So the chord-based quantum botnet owns better robustness and stability.

5. Conclusion

The control platform of chord-based quantum botnet is constructed based on the principle of quantum secure communication in order to make it better achieve the periodic update of routing table and to avoid the tracking of security devices. The in-depth analysis showed that the infected hosts in the chord-based quantum botnet can more quickly be increased, and can maintain a larger scale compared with the traditional chord-based botnet. So the chord-based quantum botnet owns better robustness and stability.

Acknowledgements

This paper is supported by the National Natural Science Foundation of China (Grant No. 41074090), Doctor Fund of Henan Polytechnic University (Grant No. 648735) and Henan Province Open Laboratory for Control Engineering Key Disciplines (Grant No KG20 09-20).

References

[1] Grizzard JB, Sharma V, Nunnery C. Peer-to-PeerBotnets: Overview and Case Study. In Proc. of the 1stWorkshop on Hot Topics in Understanding Botnets (Hot—Bots 2007). Boston. 2007.

[2] Ying Ling-yun, Feng Deng-guo, Su Pu-rui, P2P-Based Super Botnet:Threats and Defenses, ACTA ELECTRONICA SINICA. 2009.

[3] François Jérôme, State Radu, Festor Olivier. *Towards malware inspired management frameworks.* IEEE/IFIP Network Operations and Management Symposium. 2008.

[4] Chen Lu-Ying, Wang Xin-Liang, Zhao Xin, et al. *Research of botnet anomaly detection algorithm based on private protocol.* Proceedings of 2010 3rd IEEE International Conference on Broadband Network & Multimedia Technology. 2010; 55-59.

[5] Wang Xin-Liang, Lu Nan, Wang Cui-Cui. *Research of botnet detection based on multi-stage classifier.* Proceedings of the 2011 International Conference on Electrical, Information Engineering and Mechatronics. 2011; 1463-1472.

[6] Lu Nan, Wang Xin-Liang, Liu Fang, et al. Research of the combined botnet detection method based on random subspace. 4th IEEE International Conference on Broadband Network and Multimedia Technology. 20116; 15-619.

[7] Ma Xiao-Bo, Guan Xiao-Hong, Tao Jing, et al. *A novel IRC botnet detection method based on packet size sequence*. IEEE International Conference on Communications. 2010; 1-5.

[8] Genevieve Bartlett, John Heidemann, Christos Papadopoulos. *Low-rate, flow-level periodicity detection*. 2011 IEEE Conference on Computer Communications Workshops. 2011; 804-809.

[9] Bennett CH, Brassard G. *Quantum cryptography; Public-key distribution and coin tossing.* Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. 1984; 175-179.

[10] Ekert AK. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.,* 1991; 67(6): 661-663.

[11] Bennett C H, Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.,* 1992; 68(21): 3121-3124.

[12] Goldenberg L, Vaidman L. Quantum Cryptography based on Orthogonal States. *Phys. Rev. Lett.,* 1995; 75: 1239-1243.

[13] Beige A, Englert BG, Kurtsiefer C, et al. Secure communication with a publicly known key. *Acta Phys Pol A*. 2002; 101(3): 357-368.

[14] Bostrom K, Felbinger T. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.,* 2002; 89(18): 7902-7905.

[15] Deng Fu-Guo, Long Gui-Lu, Liu Xiao-Shu. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A.,* 2003; 68(4): 042317-042324.

[16] Deng Fu-Guo, Long Gui-Lu, Secure direct communication with a quantum one-time pad. *Phys. Rev. A*. 2004; 69(5); 1-4.
[17] Ba An Nguyen. Quantum dialogue. *Phys. Lett. A*. 2004; 328(1): 6-10.
[18] Sameh El-ansary, Luc Onana Alima, Per Brand, Seif Haridi. *Efficient Broadcast in Structured P2P Network.* In 2nd International Workshop on Peer-to-Peer Systems. 2003.