International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.347-354
http://dx.doi.org/10.14257/ijsia.2016.10.4.31

Trusted Quantum Botnet Research based on Dual-Chord Protocol

Wang Xin-Liang, Fu Meng-Meng

School of Electrical Engineering and Automation, Henan Polytechnic University, junci158@163.com

Abstract

The controller in the traditional chord-based botnets needs to maintain the periodic communication among all the adjacent peerbots so that every peerbot could efficiently master the new routing information. Once some peerbot is captured by the anti-virus software and is treated as a honeypot, the security personnel can capture more peerbots by tracking the deployed honeypot when it updates the routing table so that the robustness of botnet would be affected. To solve the above-mentioned problem, the trusted chord-based quantum botnet is proposed that utilizes the quantum secure channel to achieve the updating of routing table, and introduces the anti-tracking network for capturing the deployed honeypots. The anlysis result showed that the robustness and stability of trusted chord-based quantum botnet could efficiently be improved.

Keywords*: dual-chord, quantum botnets, periodic communication, anti-tracking network*

1. Introduction

Botnet [1] is a group of compromised computers controlled by the control server, and has caused a great threat on network security, information security and national security. The traditional centralized botnet owns better control efficiency; however there exists the single point of failure. So the p2p-based botnet(for example: chord-based botnet) is improved to solve the above problem, and it owns the distributed control structure that makes the detection and tracking of botnet more difficult. However, the proactive detection method can capture the p2p-based botnet, and can obtain the related information of control commands and channels through a variety of manners, and then joins the botnet to observe and monitor the internal activities. Bacher, Holz *et al* [2, 3] captured a large number of bot program by deploying the second-generation honeynet. Snort_inline is used to analyze control commands that some host will join the botnet to track and obtain more information by utilizing the obtained control information.

Rajab *et al* [4] proposed a method of tracking a large number of botnet from multiple perspectives, made a in-depth analysis of the bot program, and conducted the in-depth research on the behavior of botnets.

In 2005, the BeiJing University started to implement the honeynet in the network to track the botnets. It utilized the honeynet and sandbox technology to analyze the captured malware in order to confirm whether the malware was a bot program. Eventually, about 60000 bot samples were obtained, and more than 500 active botnets were tracked. Their home country distribution, size distribution, and other information were made the detailed statistics. So, the honeypot technology is an efficient manner to detect the p2p-based botnet including the chord-based botnet. Meanwhile, the controller in the chord-based botnets needs to maintain the periodic communication among all the adjacent peerbots so that every peerbot could efficiently master the new routing information. The security personnel can capture more peerbots by tracking the deployed honeypot when the honeypot updates the routing table, and the network security devices can also track the traffic of periodic communication to detect botnet [5] so that the robustness [6-10] of

ISSN: 1738-9976 IJSIA

botnet would be affected. To solve the above-mentioned problem, the quantum secure channel will be established to achieve the updating of routing table, and the anti-tracking network will be introduced for capturing the deployed honeypots so that the robustness of botnet could be improved.

The quantum secure channel can make botnet from eavesdropping. In 1993, Bennett *et al* proposed that quantum teleportation [11] could be achieved by using the quantum entanglement. In 1997, Bouwmeester *et al* established the quantum channel by using entangled photons, and eventually finished the first quantum teleportation [12]. The multi-particle quantum teleportation and controlled quantum teleportation were respectively proposed in the literatures [13-16]. The literature [17-18] construct the communication protocol in link layer based on quantum entanglement that could effectively improve the protocol performance. So if the quantum channel is used for periodic communication in the chord-based botnet, it will efficiently avoid the eavesdropping. However, the quantum channel can not avoid the tracking of honeypot.

To solve this problem, a control platform will be constructed by the anti-tracking network and quantum channel, so that it could not only detect the eavesdropping , but also capture the deployed honeypot. In total, the new control platform of quantum botnet can efficiently improve the security of botnets.

2. Trusted Chord-Based Quantum Botnet

The chord-based quantum botnet can realize the update of routing table between the peerbots and can avoid the tracking of security devices. However, if some peerbot was captured by the anti-virus software, the network security personnel could not remove it immediately, but as a honeypot. When the honeypot updated the routing table, the network security personnel could capture the other peerbots by tracking the honeypot traffic. So, it is important how to avoid the tracking detection of honeypot in the chord-based quantum botnet. In this paper, the trusted botnet is proposed to solve the above problem by utilizing dual-chord protocol and quantum entanglement.

The trusted quantum botnet is mainly composed of chord-based quantum botnet module and anti-tracking module. It establishes the quantum secure channel between the peerbot and its adjacent nodes by using the quantum teleportation in the chord-based quantum botnet module, as shown in Figure 1. Meanwhile, in order to void the tracking, the trusted peerbots will constitute a new anti-tracking network to remove the honeypot. Specific functions are as follows:

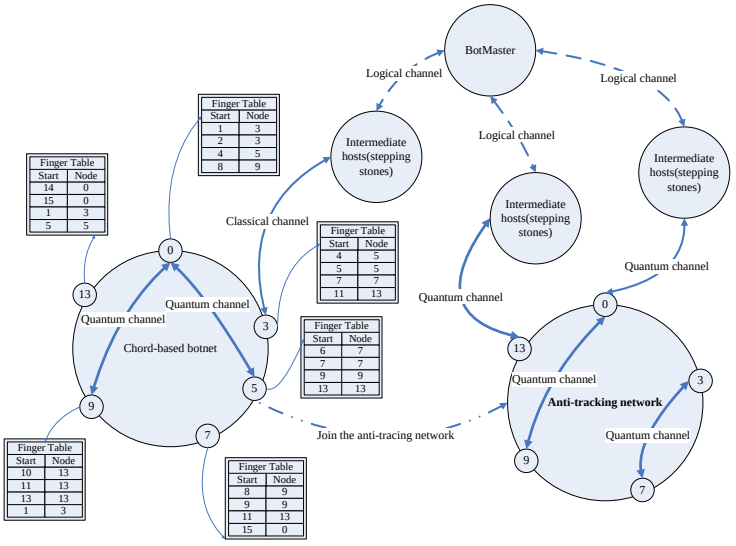

Figure 1. Network Topology of Trusted Quantum Botnet based on Dual-Chord Protocol

2.1. Trusted chord-based Quantum Botnet Module

2.1.1. The Routing Information Updating : The periodic communication packets need to be sent between the adjacent peerbots, so that each peerbot could master the current routing information. If the classical channel is directly used to transfer the routing table, once the routing information is eavesdropped, it will lead to exposure a large number of peerbots. So the module will construct the secure quantum channel to transfer the data. The works are as follows:

Assuming that the node i needs to exchange the routing table with the adjacent node $i+1$, EPR entangled particles j and $j+1$ will be assigned between the node i and $i+1$. The particle j will be assigned to the node i, and the particle $j+1$ will be assigned to the node $i+1$.

After the peerbot i is online, it will firstly join the chord-based botnet, and obtain the latest routing information. In fixed time interval or non-fixed time interval, the adjacent peerbot $i+1$ will encode the routing information according to encoding table shown in Table 1, and will prepare the particle $j+2$ that is represented by $a|0\rangle+b|1\rangle$, and $a^2+b^2=1$. Then, the particles $j+2$, j and $j+1$ will constitute a joint system.

Assuming that $|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)$, $|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)$, Then

$$(a|0_{j+2}\rangle+b|1_{j+2}\rangle)\otimes(\frac{1}{\sqrt{2}}(|0_{j+1}0_j\rangle+|1_{j+1}1_j\rangle))$$

$$=\frac{1}{\sqrt{2}}(a|0_{j+2}0_{j+1}0_j\rangle+a|0_{j+2}1_{j+1}1_j\rangle+b|1_{j+2}0_{j+1}0_j\rangle+b|1_{j+2}1_{j+1}1_j\rangle)$$

$$=\begin{aligned}&\frac{1}{2}a|0_j\rangle(|\phi^+_{j+2,j+1}\rangle+|\phi^-_{j+2,j+1}\rangle)+\frac{1}{2}b|1_j\rangle(|\phi^+_{j+2,j+1}\rangle-|\phi^-_{j+2,j+1}\rangle)+\\&\frac{1}{2}a|1_j\rangle(|\psi^+_{j+2,j+1}\rangle+|\psi^-_{j+2,j+1}\rangle)+\frac{1}{2}b|0_j\rangle(|\psi^+_{j+2,j+1}\rangle-|\psi^-_{j+2,j+1}\rangle)\end{aligned}$$

$$=\begin{aligned}&\frac{1}{2}|\phi^+_{j+2,j+1}\rangle(a|0_j\rangle+b|1_j\rangle)+\frac{1}{2}|\phi^-_{j+2,j+1}\rangle(a|0_j\rangle-b|1_j\rangle)+\\&\frac{1}{2}|\psi^+_{j+2,j+1}\rangle(a|1_j\rangle+b|0_j\rangle)+\frac{1}{2}|\psi^-_{j+2,j+1}\rangle(a|1_j\rangle-b|0_j\rangle)\end{aligned}$$

The particles $j+2$ and $j+1$ will be measured by Bell basis. After measuring, the particle j will collapse into one of following four states that are represented by $a|0_{3i}\rangle+b|1_{3i}\rangle$, $a|0_{3i}\rangle-b|1_{3i}\rangle$, $a|1_{3i}\rangle+b|0_{3i}\rangle$ and $a|1_{3i}\rangle-b|0_{3i}\rangle$, and the measuring result will be sent to the node i for exchanging the routing information. When the node i receives the measuring result, it will perform the transformation on the particle j and can obtain the transferred information on particle $j+2$. The transformation factor is shown in Table 2, and $I=\begin{vmatrix}1&0\\0&1\end{vmatrix}$, $\sigma_z=\begin{vmatrix}1&0\\0&-1\end{vmatrix}$, $\sigma_x=\begin{vmatrix}0&1\\1&0\end{vmatrix}$, $\sigma_y=\begin{vmatrix}0&1\\-1&0\end{vmatrix}$. Finally, the node i will obtain the routing information of adjacent node by decoding the particle j according to encoding rule

Table 1. Encoding Rule

No.	Polarization state	Classic bits
1	$\|\square\rangle$	0
2	$\|\square\rangle$	1

Table 2. Measurement Results of Particles

No.	Measurement results of $j+2$ and $j+1$	Quantum state of j	Transformation factor
1	$\|\phi^{+}_{3i-2,3i-1}\rangle$	$a\|0_{3i}\rangle+b\|1_{3i}\rangle$	I
2	$\|\phi^{-}_{3i-2,3i-1}\rangle$	$a\|0_{3i}\rangle-b\|1_{3i}\rangle$	σ_z
3	$\|\psi^{+}_{3i-2,3i-1}\rangle$	$a\|1_{3i}\rangle+b\|0_{3i}\rangle$	σ_x
4	$\|\psi^{-}_{3i-2,3i-1}\rangle$	$a\|1_{3i}\rangle-b\|0_{3i}\rangle$	σ_y

2.1.2. Releasing the Control Command: In trusted chord-based quantum botnet, each existing peerbot can be used to release the control command, and every peerbot is equally important. When the controller needs to release the commands, it will randomly select some peerbot to broadcast the control command [19]. After the selected peerbot receives the commands, it will send the commands to all adjacent peerpots that will continue to transmit the commands to their adjacent peerbots until that all peerbots could receive the control commands.

2.1.3. Joing and Leaving of Nodes: The peerbot in the botnet may join or leave at any time. When the host B is infected by the peerbot A, A will send local routing table to the host B, and the infected host B will join the chord-based botnet by the peerbot A. The specific process is as follows:

1) Looking through the predecessor and successor of B by the peerbot A;
2) The host B joins between the predecessor and successor;
3) Initializing the routing table of host B, and updating the routing information of other nodes.

2.2. Chord-based Quantum Anti-Tracking Module

2.2.1. Anti-Tracking Network: The each node in the anti-tracking network is trusted, and is used to distinguish whether some node has been captured as a honeypot. The specific content is as follows:

1) Anti-tracking network also uses the chord protocol to achieve the effective management, and its process of routing table updating is same as the chord-based quantum botnet module.
2) The node selection of anti-tracking network. In the first stage, some trusted nodes will be deployed in the network to distinguish the comprised nodes. If some comprised node is ensured as a honeypot, it will be removed from chord-based quantum botnet to ensure the botnet security. In the second stage, when Chord-based quantum botnet reaches a certain scale, the anti-tracking network will face a problem that there are not enough trusted nodes to distinguish the nodes in the chord-based quantum botnet. For

solving the above problem, some new nodes of anti-tracking network will be recruited. The recruiting rule is as follows:

- The trusted node needs to own the static IP, and can maintain the longer online time.
- The trusted node owns the bigger bandwidth that can be used for detecting more captured honeypots.
- The trusted node must pass the test of anti-tracking network.

2.2.2. The Distinguishing Process: The botmaster will randomly select some zombie hosts to distinguish whether they has been controlled by the network security personnel. The specific process is as follows:

1) The botmaster will releasing the control command to the zombie host i, and the control command includes the relative attack parameters that are individually the attack rate, attack duration, attack type and attack destination.
2) When the zombie host i receives the attack command, if it has been controlled by the network security personnel, it will only analyze the command, and will not perform the attack command to damage the network security. Instead, if the peerbot is still trusted, it will launch the attack immediately.
3) When the attacked node suffers the attack, it will capture all the attack traffic to analyze, and obtain the attack indicators. After the attack terminates, it will send the attack result to the botmaster.
4) When botmaster receives the attack result, it will decide whether the zombie host i is trusted.

3. Performance Analysis

In this paper, the work process of above botnets will be described by the improved SIR model. In the traditional chord-based botnet, if the peerbot is captured by the anti-virus software, the network security personnel possibly treats it as a honeybot to track the other peerbots. For the peerbot needs to update the routing table, its adjacent nodes will quickly be captured. The improved SIR model is described by the following equations:

Assuming that $N(t)$ is the largest number of hosts at time t in the chord-based botnet, $I(t)$ is the number of infective hosts at time t, $S(t)$ is the number of susceptible hosts, $R(t)$ is the number of recovered hosts at time t, β is the infection rate in the period, γ is the immune rate in the period, ∂ is the number of infected peers that the security devices can capture by tracking some captured honeypot, and $\partial < m$.

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

In the trusted chord-based quantum botnet, for it introduces the trusted anti-tracking network to detect the honeypot, it can effectively avoid that more adjacent peerbots are captured. However, in the anti-tracking network, the trusted peerbots need to be selected from the chord-based quantum botnet, so it will affect the scale of chord-based quantum botnet and will reduce the number of spreading nodes. The trusted chord-based quantum botnent can be described by the following equations:

Assuming that ε is the rate that the infective hosts of $I(t)$ can be used as the trusted nodes in the period, $AT(t)$ is the number of trusted nodes at time t, P is the probability

that the captured honeypot can be detected by the anti-tracking network. For there are limited nodes in the anti-tracking network, it is impossible to track all the nodes in the chord-based quantum botnet.

$$\frac{dI(t)}{dt} = (1-\varepsilon)\beta S(t)I(t) - \gamma(1-\varepsilon)I(t) - \partial(1-P)\gamma(1-\varepsilon)I(t)$$
$$\frac{dS(t)}{dt} = -(1-\varepsilon)\beta S(t)I(t)$$
$$\frac{dAT(t)}{dt} = \varepsilon I(t)$$
$$\frac{dR(t)}{dt} = (1-\varepsilon)\gamma I(t) + \partial(1-P)\gamma(1-\varepsilon)I(t)$$
$$N(t) = I(t) + S(t) + R(t)$$

Assuming that $N(t)=2^m$, $m=20$, $I(0)=10$, $S(0)=2^{20}-I(0)=2^{20}-10$, $\beta=0.05/N(t)$, $\gamma=0.004$, $\partial=m/2=10$, $\varepsilon=0.2$, $P=0.2$, $I(t)$ in the above botnets is shown in Figure 2, 3. From Figure 2, the infected hosts $I(t)$ in the traditional chord-based botnet can more quickly be increased, however its scale will quickly decrease for the network security device can detect more peerbots by tracking the captured honeypot. The infected host $I(t)$ in the trusted chord-based quantum botnet can maintain a certain scale for a longer period for it can remove the captured honeypot by the anti-tracking network. From Figure 3, the susceptible hosts $S(t)$ in the trusted chord-based quantum botnet is smaller compared with the traditional chord-based botnet because the peerbots in the trusted chord-based quantum botnet isn't completely used for propagation, and a part of peerbots joins the anti-tracking network for detecting the captured honeypot. Although the trusted chord-based quantum botnet infects the less peerbot, it can assure the security of botnet, and maintain the network scale for a longer time, so the trusted chord-based quantum botnet owns better robustness and stability.

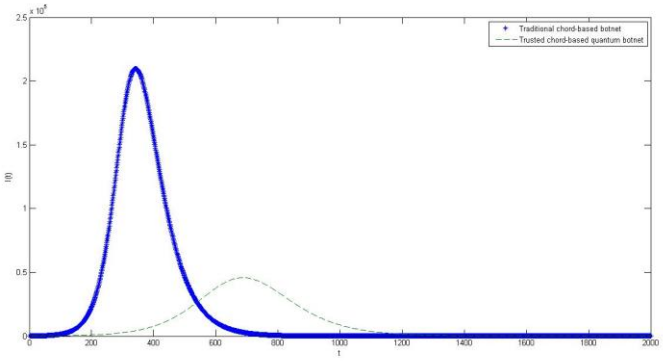

Figure 2. I(t)

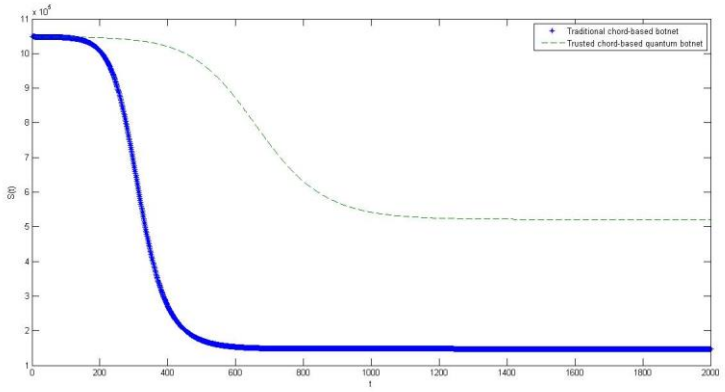

Figure 3. S(t)

4. Conclusions

The trusted chord-based quantum botnet is constructed by the anti-tracking network and the quantum secure channels, and it can effiently detect the captured honeypot by the anti-software so that it could avoid the more peerbots detected by security devices. The analysis based on improved SIR model shows that the infected host in the trusted chord-based quantum botnet can maintain a certain scale for a longer period. So the trusted chord-based quantum botnet owns better robustness and stability.

Acknowledgements

This paper is supported by the Doctor Fund of Henan Polytechnic University (Grant No B2012-073), the Key Lab of Mine Informatization, Henan Polytechnic University (KY2015-08).

References

[1] Grizzard JB, Sharma V, Nunnery C, "Peer-to-PeerBotnets: Overview And Case Study", Proceedings of the 1stWorkshop on Hot Topics in Understanding Botnets, Boston, (2007), pp. 1-8.
[2] Bacher P, Holz T, Kotter M, Wicherski G, "Know your enemy: Tracking botnets", http://www.honeynet.org/papers/bots, (2005).
[3] Freiling F, Holz T, Wicherski G, "Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks", Proceedings of the 10th European Symp. on Research in Computer Security, (2005), pp. 319-335.
[4] Rajab MA, Zarfoss J, Monrose F, Terzis A, "A multifaceted approach to understanding the botnet phenomenon", Proceedings of the 6th ACM SIGCOMM conference on internet measurement, Rio De Janeiro, Brazil, (2006), pp. 41-52.
[5] François Jérôme, State Radu, Festor Olivier, "Towards malware inspired management frameworks", Proceedings of IEEE/IFIP Network Operations and Management Symposium, (2008), pp. 105-112.
[6] Chen Lu-Ying, Wang Xin-Liang, Zhao Xin, "Research of botnet anomaly detection algorithm based on private protocol", Proceedings of 2010 3rd IEEE International Conference on Broadband Network & Multimedia Technology, (2010), pp. 55-59.
[7] 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), pp. 1463-1472.
[8] Lu Nan, Wang Xin-Liang, Liu Fang, "Research of the combined botnet detection method based on random subspace", Proceedings of 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, (2011), pp. 615-619.
[9] Ma Xiao-Bo, Guan Xiao-Hong, Tao Jing, "A novel IRC botnet detection method based on packet size sequence", Proceedings of 2010 IEEE International Conference on Communications, (2010), pp. 1-5.
[10] Genevieve Bartlett, John Heidemann, Christos Papadopoulos, "Low-rate, flow-level periodicity detection", Proceedings of 2011 IEEE Conference on Computer Communications Workshops, (2011), pp. 804-809.

[11] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A, Wootters W K, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", Journal of Phys. Rev. Lett., vol. 70, no. 13, (1993), pp.1895-1899.
[12] ouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurtor H, Zeiling A, "Experimental quantum teleportation", Journal of Nature, vol. 390, no. 390, (1997), pp.575-579.
[13] Yang C P, Guo G C, "Multiparticle generalization of teleportation", Journal of Chin. Phys. Lett., vol. 17, no. 3, (2000), pp.162-164.
[14] Braunstein S L, Kimble H J, "Teleportation of continuous quantum variables", Journal of Phys. Rev. Lett., vol. 80, no. 4, (1998), pp.67-75.
[15] Zhang X G, Li H M, Ji H, Zeng H S, "Controlled teleportation of multi-qudit quantum information", Journal of Chin. Phys., no. 10, (2007), pp.2880-2884.
[16] Zheng S. B, "Scheme for approximate conditional teleportation of an unknown atomic state without the Bell-state measurement", Journal of Phys. Rev. A, vol. 69, no. 6, (2004).
[17] Zhou NanRun, Zeng GuiHua, Gong LiHua, Liu SanQiu, "Quantum communication protocol for data link layer based on entanglement", Journal of Acta Phys. Sin, vol. 56, no. 9, (2007), pp.5066-5070.
[18] Zhou NanRun, Zeng BinYang, Wang LiJun, Gong LiHua, "Selective automatic repeat quantum synchronous communication protocol based on quantum entanglement", Journal of Acta Phys. Sin, vol. 59, no. 4, (2010), pp.2193-2199.
[19] Sameh El-ansary, Luc Onana Alima, Per Brand, Seif Haridi, "Efficient Broadcast in Structured P2P Network", Proceedings of the 2nd International Workshop on Peer-to-Peer Systems, (2003), pp. 304-314.

Authors

Wang Xin-Liang, he received the Ph.D. degree in signal and information processing from BeiJing University of Posts and Telecommunications in 2011. Now, he is a associate professor working in the school of electrical engineering and automation, Henan Polytechnic University. His current research interests include smart power grids.

Fu Meng-Meng, he is a graduate student studying in the school of electrical engineering and automation, Henan Polytechnic University. His current research interests include smart power grids and coal mine high voltage power supply grid.

