Model the P2P Attack in Computer Networks

Wei Wang *
Science and Technology on Communication Information Security Control Laboratory
Jiaxing, China, 314001
wwzwh@163.com
* Corresponding Author

Wenhong Zhao
Nanhu College
Jiaxing University
Jiaxing, China, 314001

Abstract—To analyze the distributed attack actions in computer networks, different models are discussed. Firstly, the Hybrid P2P, Pure P2P and Super P2P structures of attack are presented. The, the broadcast mechanisms of every structure are introduced. The attack methods mainly focus on the index poisoning and routing table poisoning on the general nodes and access point. By the presented model, high attack flexibility, no single point of failure, high freedom may be achieved. It is difficult to cluster, identify the attack traffic and trace the attacker. So, security researchers of computer networks should catch the attention of P2P attacks.

Keywords-P2P Attack; Attack Model; Network Throughput; Network Security; Attack Structure

I. INTRODUCTION

When the computer network is attacked, different attack methods can be performed by multiple network attack nodes. Then, how to model actions of these attacks nodes, and the efficiency analysis of their coordinated attack operations is an urgent problem for security analysis of computer networks.

This paper mainly studies how to organize multiple attack nodes to effectively attack the computer networks. Existing computer network attack systems mostly adopt a master-slave structure (centralized structure) [1-4] for attack, wherein the master attack nodes mainly develop attack strategies and issue attack rules while the slave attack nodes mainly perform specific attack. In such master-slave structure for coordinated attack with multi-nodes, the master attack nodes are easy to be found by the enemy and thus subject to "decapitate" confrontation. To avoid this problem, some implementation of more effective multi-node coordinated attack methods uses more subtle and robust multi-node attack structure. Based on the P2P structure [5-9], a new multi-node coordinated attack model is proposed in this paper. This model is advanced in attack flexibility, no single point of failure, etc., and is more suitable for security analysis of computer networks.

II. DESCRIPTION OF THE MODEL

Compared with the centralized structure, the P2P structure is more excellent in stealth and robustness. Thus, the attack P2P structure (hereafter referred to as the P2P attack network) is more difficult to detect and protect than conventional network attack systems. Besides, P2P attack network is featured in attack to the shared resources among the nodes. Each attack node in the network plays the role of attacking both the resource providers and users, and can make full use of the attack resources. Therefore, P2P attack network can provide a good distributed attack platform for the attacker for parallel implementation of a variety of attack missions.

The establishment of P2P multi-node coordinated attack model needs to solve three problems, namely link configuration, broadcast mechanism and attack methods, wherein, the link configuration means the determination of the relationship among all attack nodes in accordance with certain rules to form an overlay network; broadcast mechanism refers to rapid receipt and transfer of data, instructions and various types of attack information among the attack nodes; and attack methods refer to effective attack to target networks by making use of the features of P2P structure.

A. Link configuration

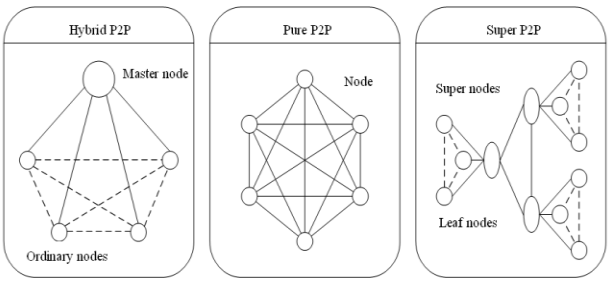

Figure 1. Three Models of P2P Attack Networks

The overall structure of the P2P attack networks can be classified as hybrid P2P, pure P2P and super P2P (see Fig. 1). Wherein, the hybrid P2P has master nodes responsible for the management, control or coordination of all ordinary nodes, and active sharing of attack resources can also be realized among ordinary nodes; all nodes in pure P2P structure have the same position, and there is no central node; and super P2P has the characteristics of both hybrid P2P and pure P2P, it is composed of the super nodes and leaf nodes, each super node has multiple leaf nodes to form a hybrid P2P structure, and a pure P2P structure will be formed among the super nodes.

Link of P2P attack networks is described in node-weighted graph (namely, nodes in the graph can be given different weights). Hybrid P2P attack network is composed of the master nodes (with weight value of 0 and called class-0 nodes) and ordinary nodes (with weight value of 0 and called class-1 nodes). All of the class-1 nodes are linked to class-0 nodes. The weight values of the nodes in

pure P2P attack network are the same (set to 0), and the link method is uncertain. Super P2P attack network also contains class-0 (super nodes) and class-1 (leaf nodes) nodes, and each class-0 node is linked with multiple class-1 nodes, all class-0 nodes are interlinked in a uncertain link mode.

Any P2P mode can be applied to P2P attack network. Such modes have their advantages and disadvantages: (a) hybrid P2P mode is easy to maintain and manage messages conveniently but there is single point of failure. The attack network-based on this mode is easy to construct due to the simple structure. In addition, the traditional attack system itself is composed of the master nodes and slave nodes, with the basic condition to be improved into hybrid P2P attack network. It can be realized just by transforming the operation mode of the nodes. (b) Pure P2P mode can avoid a single point of failure but the process to establish the network link is more complicated. The attack network based on this mode is complicated in link configuration. In terms of network access guidance, it can independently search for other attack nodes and can also get the list of neighbor nodes from other nodes; in terms of neighbor selection, the attack node information can be exchanged and randomly selected or selected according to node identifier characteristics. (c) Super P2P mode is a compromise between the first two modes. The link configuration of the attack network based on this mode includes two levels. The level of super node link configuration is equal to that of pureP2P attack networks while the leaf node level of link configuration is equal to that of the hybrid P2P attack networks after selecting corresponding super nodes. Each attack node needs to determine their own node type (super node/leaf node) according to some indicators (such as whether to have a static IP address or a higher network bandwidth, etc.).

B. Broadcast mechanism

The main purpose of the coordinated attack network with multiple nodes based on P2P structure is to perform coordinated attack on the target network by the attacker by using a large number of nodes, such as service degradation attack, routing attack, etc. During the attack, the attacker hopes that the attack commands or attack resources (called the attack synchronization information) can quickly reach other attack nodes in the P2P network after sent from any attack node, namely completion of attack synchronization among the attack nodes. Thus, P2P attack network should be equipped with fast broadcast mechanism.

For hybrid P2P attack networks, attack commands and attack resources can be achieved by the master nodes, and in this case the attack nodes can complete attack synchronization in a short time.

For pure P2P attack networks, flooding, BCRM and other methods can be used for attack synchronization.

Flooding is a broadcast mechanism which is widely adopted. The steps are as follows: when receiving the attack synchronization information for the first time, each attack node will forward such information to all neighbor attack nodes except the sender, and the same information received subsequently will be ignored. Flooding mechanism is simple and fast in coverage, and the deficiency lies in much communication overhead. Assuming that the total number of nodes in the network is N and the average number of neighboring nodes is k, the communication overhead is proportional to forwarding number, and the communication overhead in flooding protocol is:

$$C=N(k-1)+1 \tag{1}$$

BCRM (Blind Counter Rumor Mongering) mechanism includes the steps as follows: 1) when receiving the attack synchronization information, each attack node will forward such information to B randomly selected neighbor nodes without information exchange ever before. 2) The same attack synchronization information can be forwarded for F times at most, and the same information received subsequently will be ignored. BCRM mechanism can achieve high coverage of nodes while maintain low communication overhead. Although it is unable to get the accurate representation of the communication overhead of this mechanism, its limit is as follows:

$$C\leq NBF \tag{2}$$

DRM (Deterministic Rumor Mongering) mechanism is targeted at the degree of the known neighbor attack nodes of each attack node in P2P attack networks. This protocol takes advantage of the local P2P attack network topology information, and it is possible to further improve the broadcast performance of synchronized attack information. The steps are as follows: 1) when receiving attack synchronization information, each attack node will forward the information to all nodes of degree of 1 and B neighbor nodes with the minimum degree and without information exchange ever before. 2) The same attack synchronization information can be forwarded for F times at most, and the same information received subsequently will be ignored. By the above operation, DRM mechanism can ensure attack synchronization information broadcast performance and greatly improve the coverage of the P2P attack network.

For super P2P attack networks, broadcast of leaf nodes is performed by corresponding super nodes while the super node level of broadcast is similar to that of pure P2P networks.

Pratik Biswas et al from Stanford University proposed Semidefine Programming algorithm [10], which is targeted at the sensor nodes with the ranging function. The distance information among the nodes is the geometric constraints for the estimated location of the unknown nodes. For the two nodes i and j, assuming their coordinates as x_i and x_j and assuming the distance between two nodes as d_{ij}, when d_{ij} is smaller than the communication radius R of the nodes, the relationship between the two nodes can be expressed as:

$$\|x_i-x_j\|^2=\delta_{ij}{}^2+a_{ij} \tag{3}$$

Wherein, δ_{ij} represents correct estimates and a_{ij} represents ranging error of the sensor nodes. In this case, positioning can be regarded as the optimization of the minimum sum of all errors of the objective function, wherein the decision variables are the coordinates of the network nodes in 2*n dimensional matrix $X=[x_1x_2\ldots x_n]$. Limited by the node spacing,

$$\min\left(\sum_{i,j\in N,i<j} a_{ij} + \sum_{k,j\in N} a_{kj}\right) \quad (3)$$

global optimum value of the objective function $\min\left(\sum_{i,j\in N,i<j} a_{ij} + \sum_{k,j\in N} a_{kj}\right)$ should be calculated. The optimal solutions to appropriate decision variables are the estimated location of the nodes.

C. Attack methods

During network attack, it is generally related to the following four basic issues: 1) to obtain the attack resources; 2) to produce a moderate attack traffic; 3) to guide the attack traffic of the victims; and 4) the robustness of the attack schemes under counter conditions.

The P2P attack network model can be more properly address these issues:

1) High degree of freedom of the attack nodes to realize attack information synchronization with a lot of attack nodes in a short time so as to obtain sufficient resources to attack.

2) A lot of attack nodes widely distributed, wherein attack traffic is not easy to cluster and identify.

3) Rapid spread of attack instructions in P2P attack networks, wherein it is difficult to trace the attacker.

4) The excellent robustness of P2P structure.

P2P attack network can realize a variety of common network attacks. Fig. 2 shows the schematic of some attack methods[11].

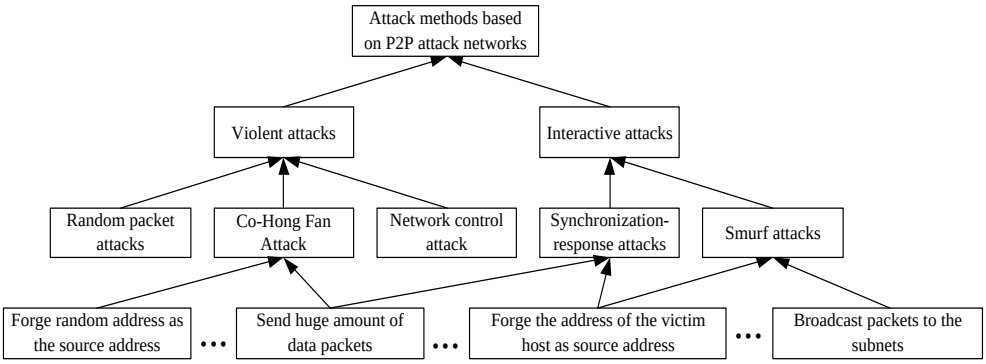

Figure 2. Schematic of common attack methods

In addition to common types of attacks, P2P attack network can also perform specific attacks against computer networks, such as index poisoning and routing table poisoning attacks, etc.

Index poisoning. Most large-scale computer networks adopt indexing technology to map network resource identifier to the corresponding node address (including port number) to facilitate access to network resources. Index can be either centralized or distributed, and the nodes participating in distributed index are called the index nodes. Each index node has some index records (called local index), and the overlap may occur among local index of different index nodes. Index poisoning refers to that the attacker inserts forged index records into the local index of each index node, wherein the node address of the forged records is the address of the attacked node. After poisoning of the index nodes, when other nodes query the node address of a certain network resource, it may get forged node address and attempt to access the address to access network resources so that the attacked node will receive invalid service requests. If there are many nodes trying to access the attacked in a short time, it may result in a network attack.

Routing table poisoning. In the computer networks, the nodes establish routing link according to node identifiers. Each node has a set of neighboring nodes. The list of these neighboring nodes constitutes the routing table of such node, wherein each item of the list contains the identifier and address of the neighbor nodes. When receiving the query request, the routing node will establish its own routing table, which will be updated with addition or exit of other nodes. Routing table poisoning refers to that the attacker manages to add forged neighbor node information to the routing table of routing nodes, wherein the node address in the forged information is the address of the attacked host. After a routing node is poisoned, when it forwards the query request, it may choose to send the message to the forged neighbor node, namely the attacked node. If the routing tables of many nodes are subject to poisoning, sending a large number of messages in a short time to the attacked node may result in a network attack.

Implementation of the above two attacks to computer networks by coordinated attack with multi-nodes of the master-slave structure is subject to the following problems: (1) it needs to use the same attack information to modify multiple network nodes information, such as index nodes and routing nodes. Such attack information is sent from the master nodes to the slave nodes to attack so that it is easy to be found by the intrusion detection system of computer networks. (2) The rapid change of routing of computer networks requires that the attacker should quickly attack. However, in centralized network, after discovery of routing update by the slave nodes, it is required to report this information to the master nodes, which will then develop new attack rules and then issue to multiple slave nodes. It results in that the attack operation is relatively slower than routing updating, thereby failing to be applicable to computer network attacks.

The P2P attack networks can avoid these problems. For example, it can send attack information from any node, and any node can specify attack rules. Thus, it can be effectively used for index poisoning and routing table poisoning attacks to computer networks.

The main attack methods are as follows:

(a) Attack to one or several nodes: As shown in Fig. 3, the attacker intercepts the RTS frame and modifies the

"duration" field according to the "type " field, and then transmits an RTS frame to the target node to inform that data is being transmitted in the current wireless network to perform the backoff process so that the target node cannot transmit data within a certain period. Attacked nodes perform the normal backoff process, with no abnormal behavior. Due to the failing of receiving the RTS frame, other nodes can perform normal communications. Overall, the network communication is normal. This attack is not easy to detect and can also facilitate the further wireless injection attacks to the target node.

(b) Attack to access points: as shown in Fig. 4, the wireless network access points and other network nodes compete for the same common channel. Thus, the RTS frame with modified "duration" field can be resent to network access points to execute the backoff process. In the attack process, the network access point cannot send data so that it cannot respond to requests to all nodes. Thus, all nodes are automatically disassociated with the network access point so that the entire network cannot communicate.

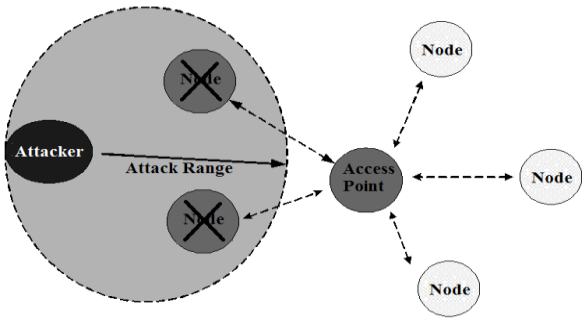

Figure 3. Attacks to nodes

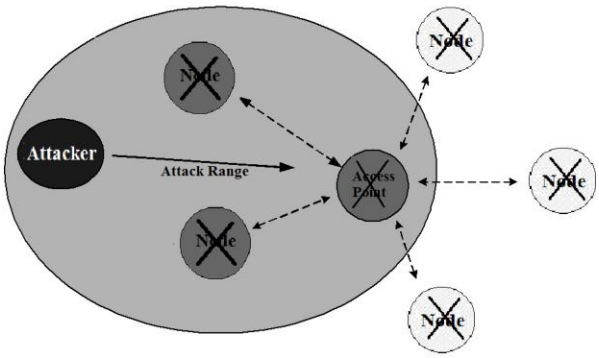

Figure 4. Attacks to the network access point

The probability for the attacker to successfully preempt the channel: the minimum channel contention window is set to CW, the number of network nodes to n and the maximum retransmission time of frame to r. Network nodes are under binary exponential backoff mechanism. The attacker always selects No. 0 contention window. Therefore, only the node which suffers the first collision with the attacker may suffer the second collision. After the first frame, the attacker will send immediately a second frame. Therefore, the NAV of the nodes suffering no collision at the first time will not be reduced by 1 for the second frame, and only the nodes suffering the first collision may select No. 0 window randomly.

As can be seen from Fig. 5, in normal communication, the load of attack by non P2P structure is much higher than the presented method.

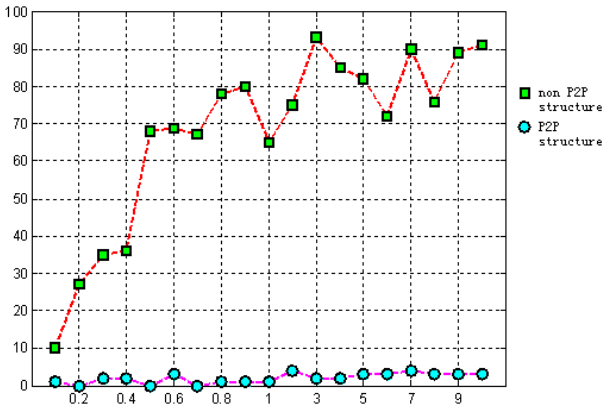

Figure 5. Communication load by different methods

III. CONCLUSIONS AND FUTURE WORK

Based on P2P structure [5-8], a new multi-node coordinated attack model for computer networks is proposed in this paper. This model is advanced in high attack flexibility, no single point of failure, high freedom in node attack, difficult to cluster and identify the attack traffic, difficult to trace the attacker, robustness, etc., and it is suitable for security analysis of computer networks. However, in terms of the above multi-node coordinated attack model based on the P2P structure, little consideration is taken into the problems which frequently occur in multi-node coordinated attack, such as jitter (joining and leaving), differentiation of the attack nodes. Our next work will focus on the establishment of theoretical model of multi-node coordinated attack targeting at the dynamical changes and differentiated features of attack nodes in computer networks by extending the above multi-node coordinated attack model based on P2P structure.

REFERENCES

[1] S.Y. Sun and Y.M. Li, "Research on Centralized Network Selection in Wireless Heterogeneous Access Network," Computer Applications, vol. 30, pp. 1163-1165, 2010.

[2] J. Chen and B.S. Yi, "Centralized Optimized TDMA Scheduling Scheme for Wireless Sensor Networks," Systems Engineering and Electronics, vol. 32, pp. 200-204, 2010.

[3] L. Fei, C.J. Pan and H.Y. Tan, "Design and Realization of Split-MAC Scheme in Centralized WLAN Network," Computer Engineering, vol. 33, pp. 112-115, 2007.

[4] K. Chen, H. Li and C.J. Pan, "Research on Radio Resource Management of Centralized WLAN Network," Computer Engineering, vol. 33, pp. 124-129, 2007.

[5] K. Kang and M. Zhang, "Analysis and Design of Distributed Network Monitoring System," Digital Technology and Applications, vol. 6, pp. 45, 2010.

[6] P.C. Su, "Design and Implementation of Distributed Network Access Control," Journal of Guizhou Normal University (Natural Sciences), vol. 26, pp. 100-103, 2008.

[7] G. Wang, F. Huang and D.X. Ming, "Research on Distributed Network Clock Synchronization," Chinese Journal of Scientific Instrument, vol. 29, pp. 2399-2403, 2008.

[8] M. Li and Y.Y. Liu, "Comparison of Three Wireless Distributed Networks," Telecommunications Science, vol. 23, pp. 95-98, 2007.

[9] T. Rohmer, A. Nakib and M.A. Nafaa, "Priori Knowledge Guided Approach for Optimal Peer Selection in P2P VoD Systems", IEEE Transactions on Network and Service Management, vol.11, No. 3, pp. 350-362, 2014.

[10] P. Biswas, Y.Y. Ye, "Semidefinite Programming for Ad Hoc Wireless Sensor Network Localization," in the proceeding of Third International SymPosium on Information Proeessing in Sensor Networks. NewYork: Academic, 2004, pp. 46-54.

[11] P.Senthil vadivu and , K.S.Karthika, "A Survey On Botnet Detection Approaches In Peer-To-Peer Network", International Journal of Advances in Computer Science and Technology, vol.3, No. 5, pp. 311-317, 2014