

A DDoS Attack by Flooding Normal Control Messages in Kad P2P Networks

Hyelim Koo^{*}, Yeonju Lee^{*}, Kwangsoo Kim^{*}, Byeong-hee Roh^{*}, Cheolho Lee^{**}

^{*}Department of Computer Engineering, Graduate School, Ajou University
San 5 Wonchon-Dong Youngtong-Gu, Suwon, 443-749, Korea
{milkystar, yjlee11, zubilan, bhroh}@ajou.ac.kr

^{**}Electronics and Telecommunications Research Institute, Korea
chlee@ensec.re.kr

Abstract—This paper introduces a new DDoS (Distributed Denial of Service) attack by flooding control messages from normal users in Kad network, which is DHT-based P2P network. The proposed attack can make normal nodes participated into the Kad network to act as if they were zombies to generate numerous control messages destined to a target system unintentionally. With the flooded control messages from those nodes, it can cause a DDoS effect to a certain system. We implemented the attacks by modifying the open source program called eMule client, and tested the impact of the proposed attack in our own constructed real Kad network test bed.

Keywords—Kad network, Kademlia, peer-to-peer (P2P), DDoS attack, Control message, eMule

I. INTRODUCTION

As networking technologies evolve, demands on large-sized multimedia data exchanges over the Internet are increased. There have been several researches to build overlay networks to send and receive files efficiently. The most popular network architecture to share information and files over the Internet is a peer to peer (P2P) network. The Kad network is the distributed hash table (DHT)-based network for P2P services. The Kad network has been one of the most popular P2P networks since DHT provides very effective routing algorithm based on logical distances rather than physical paths between peers.

There have been much of works on the attacks targeted to P2P network such node insertion[1], publish[1], eclipse[9], rational[10], routing and index poisoning[11][12], Sybil[13] attacks, and so on. Among the various attacks on P2P networks, distributed denial of service (DDoS) attacks maximally utilize the nature of the flexible and autonomous nature of P2P networks. The Kad network is more vulnerable to DDoS attacks because it allows any nodes to join the

network without any verification mechanism and its participants (or nodes) do not validate peers' IP addresses.

Locher et al.[1] discussed on the possibility of the DDoS attacks in the Kad network by using node insertion and publish attacks. However, they did not provide the detail on the attack procedure and its effectiveness. In [7], the authors introduced two DDoS attacks based on index poisoning and DHT routing table poisoning attacks, respectively. To succeed the attacks, they require very high computational complexity to alter hash values and complex procedures to carry out the attacks. In addition, it is known that current implementations for Kad applications such as eMule and aMule have defense mechanisms on those attacks.

In this paper, we propose a DDoS attack by flooding control messages from normal users in a Kad P2P network. The proposed method makes normal nodes in the network to act as if they were zombies to generate massive number of control messages destined to a victim system as in [7]. Unlike [7] based on index and routing table poisoning attacks, however, the proposed method utilizes a node insertion attack to make normal nodes to act as zombies. As mentioned before, the complexity on index and routing table poisoning attacks require very high computational complexity, while the node insertion can be implemented in a very simple and effective way. The proposed attack has been implemented by modifying the open source program called eMule client, and tested the impact of the proposed attack in our own constructed real Kad network test bed.

The remainder of this paper is organized as follows. Some related works are described in Section 2, and the proposed DDoS attack is explained in Section 3. Experimental results are given in Section 4, and finally the paper concludes in Section 5.

II. RELATED WORKS

A. Kad Network Overview

The Kad network adapts a Kademlia-based DHT routing protocol implemented by several P2P applications such as

This research was partially supported by Basic Science Research Program through the NRF of Korea funded by the MEST (2011-0025544).

Overnet, eMule, and aMule. The eMule and aMule have the largest number of simultaneously connected users since these clients connect to the eDonkey network, which is a very popular P2P system for file sharing. Compared to Chord [6], Kademlia [5] has several advantages, such as a novel XOR metric for node distance calculation, can be widely applied to eMule system and is insusceptible to several known common attacks. For these reasons, Kademlia[5] arouses wide concern nowadays.

Kad specifies the structure of a network and the exchange of information through peer lookups. Peers communicate among themselves in Kad using UDP. A virtual overlay network is formed by participating peers. Same as Chord[6], Kademlia [5] also assigns a unique NodeID in 128-bit to each node as its identity in the whole P2P network. Each peer is identified by a Kad ID. The Kad ID not only serves as an identity, but is used to locate objects. When searching for some objects, a peer needs to know the target location and explores the network in several steps. Each step will find peers that are closer to the target. The steps of the lookup procedure are following. First, a searching peer sends messages to two closest possible peers. When the searching peer received responses, it obtains three closer possible peers. Then these new possible peers that are in the target key space will be stored to a list, called a candidate list. In this example, two peers are in the target key space. These two peers will be saved to the candidate list. In the last step, the searching peer sends a request for closer peers to the three closest peers again, but only two peers are available and reply with closer peers. The lookup procedure terminates when the lookup responses contain only peers that are either already present in the candidate list or farther away from the target than the other top three candidate peers. At this point, the candidate list becomes stable. Therefore, the lookup procedure is very efficient. Furthermore, different from Chord, Kademlia takes advantage of XOR metric to calculate the distance between different nodes based on an individual NodeID. Each node maintains a routing table consisting of up to 128 kbuckets. Every bucket contains at most k contacts with (IP, UDP port, NodeID). Extended to publish or query scheme, each file will also have a unique FileID which has the same length as the NodeID. The file information will be published to the nodes that have the same or similar NodeID to FileID. In addition, to enhance the search efficiency, each node has several corresponding keywords and each keyword also has a unique hash value which constructs a key-value pair. This brilliant design provides a highly efficient publish and search scheme. However, Kademlia is weak for attack, because of following two reasons. First, it accepts all incoming message without any check mechanism. There is no restriction regarding the KadID or the IP address of the sender. With the KadID of the argnet and a good knowledge of the routing table mechanisms, it is possible to quickly take control of a legitimate peer. Second, they don't verify IP address. For implement Sybil attack, attacker needs many IDs. Attacker generates many KadIDs for one IP address. It means Attacker can make zombie nodes and control the network. Kads didn't have an ID

management policy. As a result, nodes in Kad added attacker as neighbors without doubt and it cause Sybil attack. But this attack can defend by released eMule version 0.52.

B. DDoS Attacks in Kad Network

There are two reasons that Kad network has vulnerable architecture about attack. Firstly, each node does not go through the verification process about the entire response message from other nodes in Kad network. Secondly, they do not verify the IP address in the messages. The characteristics of these Kad network is easily exploited. Typically, Kad network is attacked by node insertion attack, DHT routing table poisoning attack, and index poisoning attack. In this paper, we discuss DDoS attack especially. DDoS attacks are performed based on the aforementioned three kinds of typical attack. In the reference [7], two kinds of DDoS attacks based on poisoning (DHT routing table poisoning attack and index poisoning attack) are introduced. The former one, which called TCP-connection DDoS attack, is to overwhelm the victim's connection resource with fully-open TCP connections, thereby hampering legitimate users from making connections to the victim host. This type of attack is conducted based on index poisoning attack. The later one, which called the bandwidth DDoS attack generate enough traffic to tie up the bandwidth of the victim's access link. Also, this attack conduct based on routing table poisoning attack.

However, these attacks which behavior based on the poisoning attack cannot be realized in general. When releasing its new version, eMule updates the defense mechanism against known attacks. At the time of this writing, the problems above are fixed and patched. In addition, the complexity of the attack using poisoning is very high. Therefore, the DDoS attack through the node insertion attack we proposed is simpler and more efficient than others.

III.DDoS ATTACK BY FLOODING CONTROL MESSAGES

The Kad P2P network is basically formed with numerous nodes distributed around the world. Any node can join the Kad network without any security procedure, and the network configuration is done in an autonomous way between nodes. Due these characteristics of the Kad network, it has been exposed to various attacks including DDoS ones. Here, we describe a new DDoS attack on the Kad network. As in general DDoS attack in the Internet environments, the DDoS attack is targeted to a victim system such as an IIS (Internet Information Server). Unlike conventional Internet environment, in which attackers should find vulnerable systems and make them as zombies, any node in P2P network can be a potential attacker (or zombie) unintentionally. The victim system can be internal or external Kad network domain, while an attacker as well as the nodes to act as zombies should be in the Kad network domain.

Fig. 1 shows an overall structure for the proposed DDoS attack. To make the DDoS attack successful, attackers should carry out a node insertion attack as in [1]. When normal users search for a popular content, the Kad network provides the response faked by attackers as a result of the node insertion attack to the users. The faked response includes the victim system's information as the system that stores the content even though the system does not have it. Then, all control messages to download the content from the users are concentrated to the server. As the number of users search for the content increases, the amount of the control messages sent to the server also increases. If the number of control messages received at the server exceeds the server's capability, no service can be provided from the server.

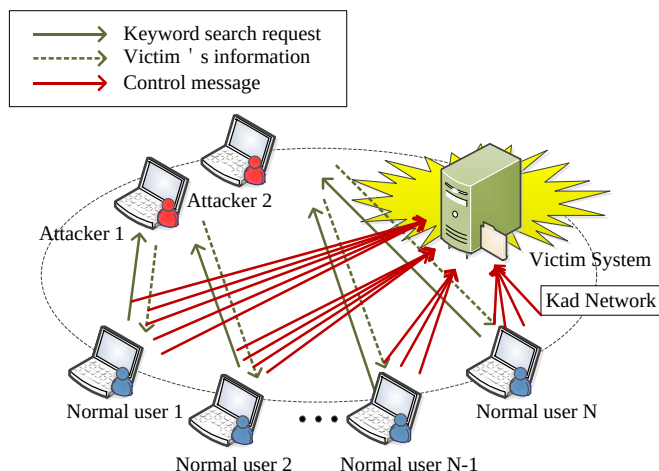


Fig. 1. Overall structure of the proposed DDoS attack

Fig. 2 shows the detail procedure for the proposed attack, which consists of four steps:

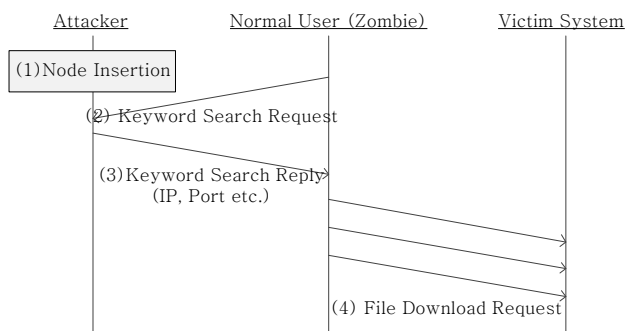


Fig. 2. DDoS Attacks through the Exchange of Control Message

- (1) Attackers join the Kad network by performing and succeeding the node insertion attack for a popular content that most P2P users are willing to search for. It is noted that it needs more than three attackers in the network to make the success rate of the attack to be larger than 95% [1].
- (2) A normal user sends Keyword Search Request with 128-bit KeywordID, which is the representation of the content to the Kad network.

- (3) Routing in the Kad network is performed based on the distance between the KeywordID and the response node's ID. The distance is obtained by the bitwise XOR of the two identifiers. As the result of the node insertion attack, the distances for the attackers are always shorter than other peers. Accordingly, the probability that the user will select the attackers' responses among others is much high. As mentioned before, the attackers' responses include the victim system's information as the system that stores the requested content.
- (4) The user tries to retrieve the download by sending File Download Request message to the victim system. Likewise, the user plays a role of zombie without its intention or any manipulation to be a zombie made by attackers.

As mentioned in [1], the DDoS attack from P2P network to the victim system outside the Kad network is much harder to detect than that in a normal DDoS attack because the IP addresses of the zombies (normal users in Kad network) are different, but valid ones. In addition, there is no erroneous operation in the Kademlia protocol, and the all incoming packets are classified as normal packets even a Firewall system monitors them.

IV. EXPERIMENTAL RESULTS

For the experiments, we constructed a test bed shown in Fig. 3 as a closed but real Kad network by using the most common open source program called eMule[8] of version 0.50 running on Windows XP PCs. We implemented the attacker by modifying the eMule client such that they perform the node insertion attack with the proposed DDoS operation. All other normal users run the original eMule client without any modification. To make the situation that numerous users join the Kad network, we have a single PC (as Botnet) run multiple eMule clients using virtual machine technique. As shown in Fig. 3, the test bed consist of two attackers, 20 Botnet PCs, one victim system, and a test PC.

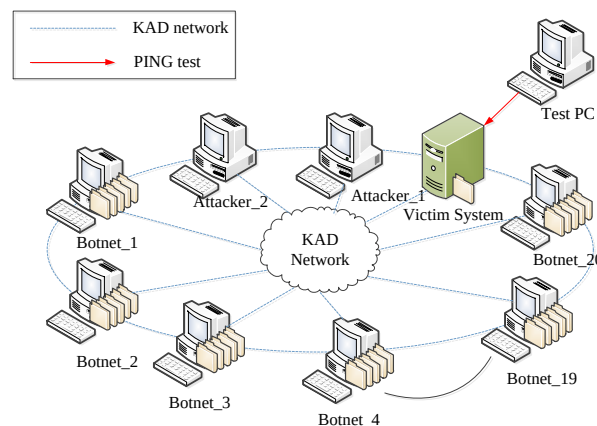


Fig. 3. Test bed for the experiments

To monitor the status of the victim server as the number of users (zombies) increases, ping tests using ICMP was conducted between the test PC and the server. It is noted that the users search the same content and the attackers provide faked information of the server for the content in the test bed environment. That is, as the number of zombies increases, the number of control messages increases also.

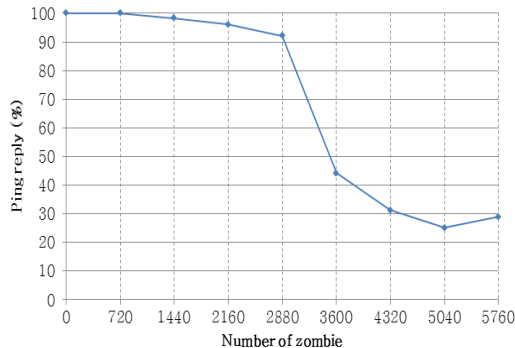


Fig. 4. Success ratio of ping request and reply (%)

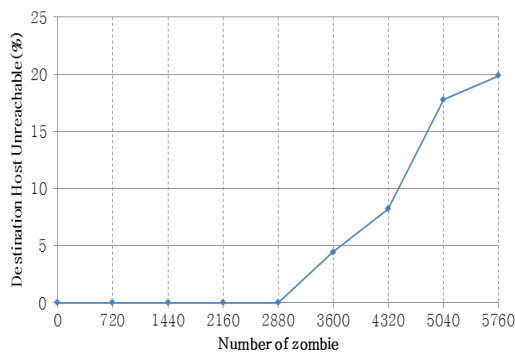


Fig. 5. Ratio of destination host (server) unreachable (%)

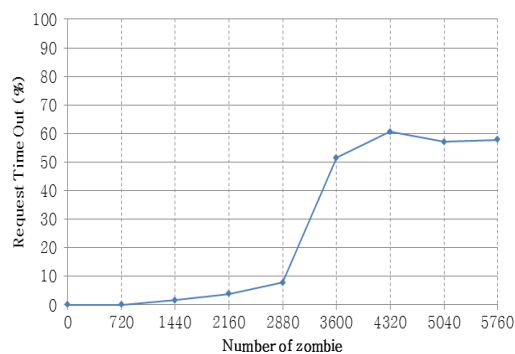


Fig. 6. Ratio of request time out (%)

Fig. 4 shows the success ratio of the ping request, which measured by the ratio of the number of successful replies to the total number of ping requests, as the number of users (zombies) increase. Fig. 5 indicates the ratio of the destination host unreachable, which means that ping requests are not arrived at the victim server. And, Fig.6 depicts the percentage of the ICMP echo request message timeout. As we can see

from Fig. 4, 5 and 6, the service performance provided by the victim system falls down sharply when the number of zombies exceeds around 2,880. The results indicate the effectiveness of the DDoS attack. That is, if there are a sufficient number of nodes on the Kad network, it can succeed DDoS attacks on a target system.

V. CONCLUSION

In this paper, we proposed a DDoS attack in Kad network, which comprises a node insertion attack and a flooding control message generation process. We showed the effectiveness of the proposed DDoS attack by constructing a test bed.

The attack can be done without any change of conventional Kademia protocol at normal users. As we mentioned before, because the attack is very hard to detect and all normal nodes in the Kad network can be a potential attacker, the impact of the attack from P2P overlay network may be more severe than normal DDoS attacks from the Internet network itself. It is expected that as P2P network users rapidly grow, the security threats in or from the P2P networks are increasing severely. So, the ways to protect the Internet as well as P2P networks should be developed and require further studies.

REFERENCES

- [1] T. Locher, D. Mysicka, S. Schmid, and R. Wattenhofer., "Poisoning the kad network," ICDCN '10, pages 195-206, January 2010.
- [2] R. Brunner and E. Biersack. "A Performance Evaluation of the Kad Protocol. Technical report, Eurecom, 2006."
- [3] Singh, A.; Ngan, T.-W.; Druschel, P.; Wallach, D. S.; , "Eclipse Attacks on Overlay Networks: Threats and Defenses," INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings, vol., no., pp.1-12, April 2006 .
- [4] T. Cholez, I. Chrisment, and O. Festor. "Evaluation of Sybil attack protection schemes in Kad," In AIMS: International Conference on Autonomous Infrastructure, Management and Security, pages 70–82, 2009.
- [5] P. Maymounkov and D. Mazieres, "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric," Peer-To-Peer Systems: First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 78
- [6] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in SIGCOMM '01. New York, NY, USA: ACM, 2001, pp. 149-160.v
- [7] Naoum Naoumov, and Keith Ross, "Exploiting P2P systems for DDoS attacks", in InfoScale '06. New York, NY, USA: ACM, 2006, pp
- [8] eDonkey network. <http://www.edonkey2000.com>
- [9] A. Singh, T.-W. J. Ngan, P. Druschel, and D. S. Wallach. Eclipse Attacks on Overlay Networks: Threats and Defenses. In Proc. 25th Annual IEEE Conference on Computer Communications (INFOCOM), 2006.
- [10] S. J. Nielson, S. A. Crosby, and D. S. Wallach. A Taxonomy of Rational Attacks. In Proc. 4th IPTPS, 2005.
- [11] J. Liang, N. Naoumov, and K. W. Ross. The Index Poisoning Attack in P2P File Sharing Systems. In Proc. 25th Annual IEEE Conference on Computer Communications (INFOCOM), 2006.
- [12] Yu, J., Li, Z. and Chen, X. Misusing Kademia Protocol to Perform DDoS attacks. Proc. ISPA 08, Sydney, Australia, IEEE Computer Society, Washington, DC. 2008 December 10–12
- [13] J. R. Douceur. The Sybil Attack. In Proc. 1st IPTPS, Cambridge, MA, March 7–8, IEEE Computer Society, Washington, DC., 2002