Attack Model and Detection Scheme for Botnet on 6LoWPAN*

Eung Jun Cho, Jin Ho Kim, and Choong Seon Hong**

Dept. of Computer Engineering, Kyung Hee University, Korea
{ejcho,jhkim}@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract. Recently, Botnet has been used to launch spam-mail, key-logging, and DDoS attacks. Botnet is a network of bots which are controlled by attacker. A lot of detection mechanisms have been proposed to detect Botnet on wired network. However, in IP based sensor network environment, there is no detection mechanism for Botnet attacks. In this paper, we analyze the threat of Botnet on 6LoWPAN and propose a mechanism to detect Botnet on 6LoWPAN.

Keywords: Botnet, 6LoWPAN, Attack Model.

1 Introduction

Attack types are varied with the development of the computer technology. In the past, attacks were launched done for just taking pride, and there was no other purpose. On 25th of January, 2003, in Korea, there was a serious attack against the Internet, it was a Slammer worm. The Slammer worm used the weak point of MS-SQL, and disabled entire network till next morning. Nowadays, attackers require money to stop attacking commercial site. According to this shifting of the attack paradigm, new kind of attack will be possible when new kind of technology is developed.

In this paper, we analyze attack case of Botnet [1][2], which is the most powerful attacking tool nowadays on 6LoWPAN (IPv6 over Low power WPAN)[3], and propose a detection mechanism of Botnet on 6LoWPAN.

2 Attack Model of Bonet on 6LoWPAN

In this section, we introduce an attack model of Botnet on 6LoWPAN. A sensor node provides low computation power, limited battery life and low bandwidth compared to that of a PC. If an attacker wants to launch DDoS(Distributed Denial of Service) attack with sensor nodes, the attacker has to infect much more number of sensor nodes than personal computer. However, although the attacker infects enough number of sensor nodes to launch DDoS attack, they cannot continue DDoS attack because of

* This research was supported by the MKE, Korea, under the ITRC support program supervised by the IITA (IITA-2009-(C1090-0902-0016)).

** Corresponding author.

C.S. Hong et al. (Eds.): APNOMS 2009, LNCS 5787, pp. 515–518, 2009.

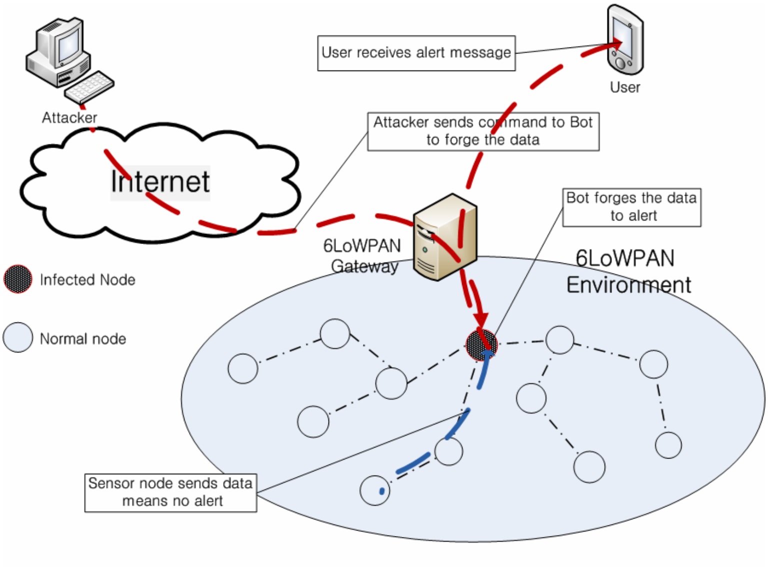
User receives alert message
User
Attacker
Attacker sends command to Bot to forge the data
Internet
Bot forges the data to alert
6LoWPAN Gateway
6LoWPAN Environment
Infected Node
Normal node
Sensor node sends data means no alert

Fig. 1. Attack model of Botnet on 6LoWPAN

the limited battery. On the other hand, the attacker can utilize one characteristic to achieve his/her goal; acts as a route of the communication. With this characteristic, the attacker can forge the data packet which is passed through infected sensor node.

Figure 1 shows the example how the attacker forges the data packet which flows to user. At first, the attacker sends command to a bot (infected node) to forge the data. After this step, the bot can try to forge the data of a packet which is passed through infected node. A user requests the temperature data to the specific sensor node. Then the sensor node replies to user that temperature is “20”. When the packet, which includes temperature data passes through infected node, the bot forges the data to “10”. Finally, the user receives the forged temperature data. So the user can turn on the heater or turn off the air conditioner to make temperature normal. If this situation is in a hospital, it can be a serious accident.

3 Detecting Mechanism for Botnet on 6LoWPAN

In this paper, we assume the following rules. First, sensor nodes use only TCP to provide the service. Second, one 6LoWPAN provides only one service. Third, procedure of the communication between sensor node and user is typical. In 6LoWPAN environment, all packets, which flow from IP network to the 6LoWPAN, have to pass through a 6LoWPAN gateway. With this characteristic, we propose a detection mechanism of Botnet on 6LoWPAN. Figure 2 shows the Botnet detection module which should be installed on the 6LoWPAN Gateway. To analysis the traffic data, we store the data from the packet that passes through the 6LoWPAN Gateway.

Control field check module calculates the sum of TCP control field during a connection. Characteristic of traffics are almost same because sensor network provides limited service. However, in case of infected node, more traffic is required to maintain Botnet and update bot module. Due to this characteristic of Botnet, the sum of TCP control field value can be different during a connection. *Packet Length check* module calculates the average packet length during a connection. Application data of packets which are sent by user and attacker are quite different. As mentioned above, bots have to transmit more data to update module and maintain Botnet. So, packets, which are sent and received by infected node, are longer than normal one. *Activity check module* counts the number of connections established by sensor node. The attacker cannot know where the bot node is. Therefore the bot has to report its state and address information to the attacker. *Activity check module* counts these connections. *Bot Analysis module* uses above information to detect whether a node on 6LoWPAN is a bot or not. First, from *Value(C)*, *Bot Analysis module* analyzes all traffic of a node to find the malicious traffic. If the malicious traffic is found, it analyzes *Value(L)* and *Value(A)* also. All values are enough to determine that there is the bot on 6LoWPAN, *Bot Analysis module* makes the alert message to manager. The following is specific operation code of *Bot Analysis module*.

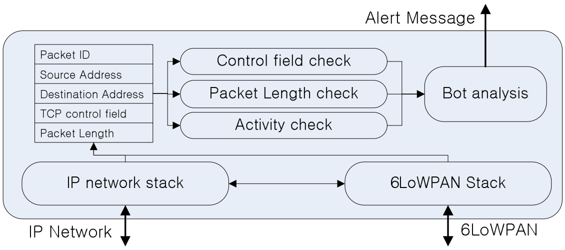

Fig. 2. Additional module on 6LoWPAN Gateway to detect Botnet

```
$Value_{c}$ : value from Control field check module
$value_{l}$ : value from Pakcet Length check module
$value_{a}$ : value from Activity check module
$value_{ci}$ : value from Control field check moudule of ith node
t : value of threshold
for(i=0; i < number of nodes; i++)
{
  if($value_{ci}$ < average $value_{c}$ of other node - $t_{1}$ &&
     $value_{ci}$ > average $value_{c}$ of other node + $t_{1}$)
    if($value_{ai}$> average $value_{a}$ &&
       $value_{li}$ < average $value_{l}$ - $t_{2}$ &&
       $value_{li}$ > average $value_{l}$ + $t_{2}$)
      Makealert();
}
```

4 Evaluation

Table 1 shows parameter and value to simulate our mechanism. And Figure 3 shows detecting rate according to value *t*, and rates of false positive according to value *t*. We vary the number of nodes to compare. To decrease rates of false positive, value *t*

Table. 1. Simulation Parameters

Parameter	Value
Random range of packet length	10~11
Number of nodes	Variable
Packet generation rate	0.5 packet per every 1ms
Random range of ACK value	5~7
Test time	400000ms
The number of simulation	100

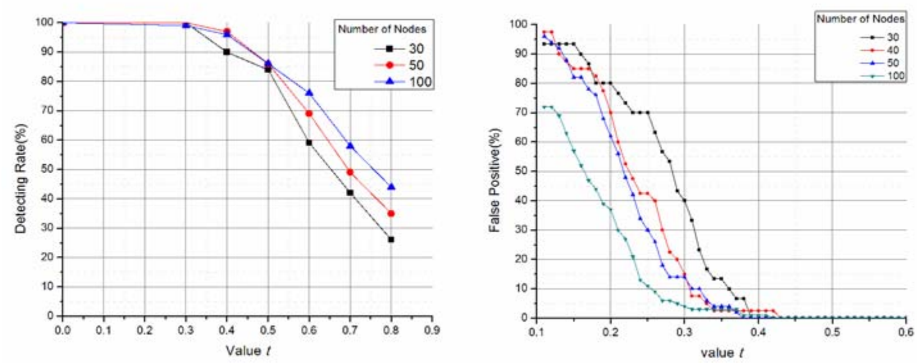

Fig. 3. False positive and detecting rate according to value *t*

should be pre-defined by doing pre-simulating. And more number of nodes makes lower false positive rates and higher detecting rates.

5 Conclusion and Future Works

In this paper, we explain the threat of Botnet attack on 6LoWPAN, and propose a detection mechanism for Botnet on 6LoWPAN. To apply our mechanism in the real sensor network, we need to consider about 6LoWPAN environment having thousands of sensor nodes and supporting multiple tasks. To reduce overheads of 6LoWPAN, we will consider sampling mechanism to analyze traffic as future works. Also, we will calculate optimal value of *t*.

References

1. Puri, R.: Bots & Botnet: An Overview, `https://cours.ift.ulaval.ca/fileadmin/cours/20064_2772A/public/Botnet.pdf` (August 2003)
2. Holz, T., Steiner, M., Dahl, F., Biersack, E., Freiling, F.: Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm, April 9 (2008)
3. Kushalnagar, N., Montenegro, G., Schumacher, C.: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, IETF RFC 4919 (August 2007)