A Study of Packet Analysis regarding a DoS Attack in WiBro Environments

D.W. Park †

†Hoseo Graduate School of VENTURE ,

Summary

This paper analyzes the DoS attack traffic on the WiBro network, generates logs and tracebacks the attacker. With attaining the integrity against the packets resulted from the malicious DoS attack, the paper provides the framework to generating forensic data. In the WiBro network environment, the attacker and the victim are the WiBro mobile terminal. The packet analyzers(Cain & Abel, Wireshark and e-Watch Lite) are used to analyze attacks. The DoS attacks are simulated by using hGod.exe and DoS 5.5. And the paper analyzes the protocols(DNS, TCP, HTTP, IP, ICMP). By showing that the time extracted from the DoS attack packets and the current time from a cellular phone are the same, the integrity is proved. The correspondence can be used the evidence for judging legal responsibility against the DoS attack.

When security accidents occur, the forensic data and the traceback data are generated. It fortifies entire Wibro network security. Future researches require real-time forensic generation and real-time traceback on Wibro IPv6.

.

Key words:

DoS, DDoS, Forensic, WiBro

1. Introduction

,

KT and SKT is enlarging WiBro (Wireless Broadband Internet) services in Seoul and the capital region and the nationwide area of Korea. WiBro is the service that a wireless Internet connection is wherever possible with high speed during movements. If you install a WiBro terminal to a PC, notebook computer, PDA or a receiver for vehicle, you can use freely the Internet like cellular phones while moving by a car or a subway. WiBro integrated terminal is able to support multi-modes such as a cellular phone and DMB.

Figure 1. The various type of WiBro

Currently a terminal of various forms is provided like Figure 1 according to user's use. WiBro provides low-speed data services such as E-mail, Display phone, E-banking, MMS (Multimedia Message Service) or SMS (Short Message Service). And high-speed data services such as VOD(Video On Demand) or downloading large data. It also provides Telematics which informs real-time traffic condition and DMB which uses multicast and broadcast techniques of a mobile internet system.

The domestic and foreign communication specialists expect that WiBro will be the core technique of NGN (Next Generation Networking). The CONCERT FORECAST 2008 report[1] published by CONCERT(Consortium of Computer Emergency Response Team) considered the six security issues in 2008. Among them DDoS(Distributed Denial of Service) attacks are the most important.

2. Related Work

2.1 WiBro(IEEE 802.16e)

WiBro Phase I was standardized by the TTA of Korea and in late 2005 ITU reflected WiBro as IEEE 802.16e (mobile WiMAX). Two South Korean Telco (KT, SKT) launched commercial service in June 2006. WiBro adopts TDD for duplexing, OFDMA for multiple access and 8.75 MHz as a channel bandwidth. WiBro Phase II standard is now being developed to harmonize with IEEE 802.16-2004 & 802.16e Draft3 or later version..

Table 1: WiBro profile

Field	Description
Spectrum	2.3GHz
Channel Bandwidth	8.75MHz
Frame Length	5ms
Multiple Access	OFDMA(Orthogonal Frequency Division Multiple Access)
Duplexing	TDD(Time Division Duplexing)
Data Rate	Uplink: 128Kbps/1Mbps Downlink: 512Kbps/3Mbps
Handoff	Inter cell, inter base station handoff handoff delay :lower than 150ms
Mobility	최대 60km/h
Service coverage	Picocell : 100m, Microcell : 400m, Macrocell : 1km

2.2 Packet Analysis

Manuscript received December 5, 2008
Manuscript revised December 20, 2008

Malicious attacks on networks or virus infections can be investigated by the packet analysis. The packet analysis is performed by the network sniffing and the protocol analysis. There are Tcpdump, OmniPeek, Cain & Abel, Wireshark to the packet analysis tools. This paper uses recent version of the Wireshark. According to wired or wireless network, WinPcap or AirPcap is used by a promiscuous mode. Minimum system requirements are CPU 400Mhz, 60MB of available hard disk space and IEEE 802.11 NIC.

2.3 DoS attack and traceback

CONCERT FORECAST 2008 report shows that DoS attack frequency increases. As shown in Figure 2., the Attacker infects handlers(reflector) by the packets which have the modified source addresses. While the attacker commands handlers to send a large volume of packets simultaneously, the victims' services are suspended. IP spoofing attack leads not to retain TCP connection by the packets which have the modified source addresses. The attacker arranges N zombie to attack the victim's system and network availability.

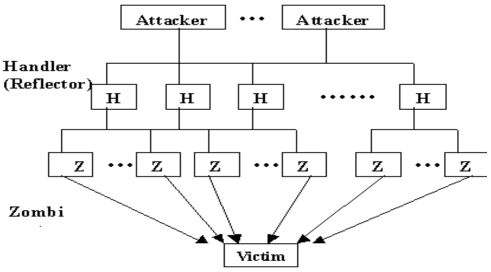


Figure 2. DoS(DDoS, DRDoS) attack model

2.4 The mobile terminal and traceback

The MAC(Message Authentication Code) makes it possible for the mobile terminal to perform access control by using authentication and the exchanges of secret keys. The MAC is comprised of three sublayers. Among the three sublayers, The Convergence Sublayer (CS) provides any transformation or mapping of external network data, received through the CS service access point (SAP), into MAC SDUs received by the MAC Common Part Sublayer (MAC CPS) through the MAC SAP.
The MAP in the MAC layer involves sending and receiving of packets, which contains the information of the traffic burst data allocation and the control messages of physical layer. The types of the MAP are Normal MAP, Compressed MAP, HARQ MAP, HARQ-support Normal MAP Extension and Sub-DL-UL-MAP. The various type of the provide location tracking, call allocation and logging. this paper makes a attained log record to forensic data and performs traceback against the mobile terminal.
The IP back-tracking actually is a traceback mechanism regarding a attacker to execute hacking through a mobile terminal. It traces back the intermediate nodes on the path between the attacker and the victim. It figures out the real source of the attack.

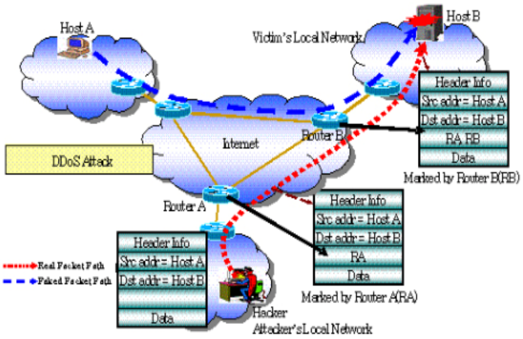


Figure 3. Traceback against DDoS attack

3. DoS attacks on WiBro environments

The various type of digital device such as PDA, Handheld PC, notebook, Smartphone can adopt WiBro for wireless communication. In this section the testbed for DoS attacks on WiBro environments is configured

3.1 WiBro environments

WiBro system structure is composed to MSS(Mobile Subscriber Station), BS(Base Station), ACR(Access ControlRouter) and Backbone.

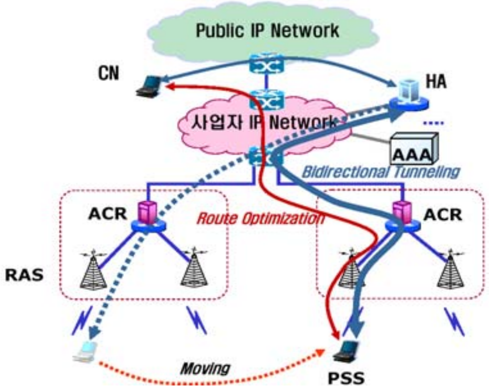


Figure 4. WiBro network

3.1.2 Connecting a WiBro mobile terminal

As shown Figure 4, in the case where the WiBro terminal has the connection with the base station and moves into another cell, if performs handoff procedures. During handoff the previous base station provides information required for authentication to the new base station.

AS shown Figure 7, If the mobile terminal recieves the MOB_BSHO-RSP and decides the target base station, if sends the MOB_HO-IND to current base station in order to nofity the initiation of the handoff. And if just performs the handoff. After transmitting the MOB_HO-IND, since the mobile terminal cannot transmmit and receive any more packets through service base stations, it should finish re-rentry procedures as soon as possible.

Figure 5. Connecting WiBro network

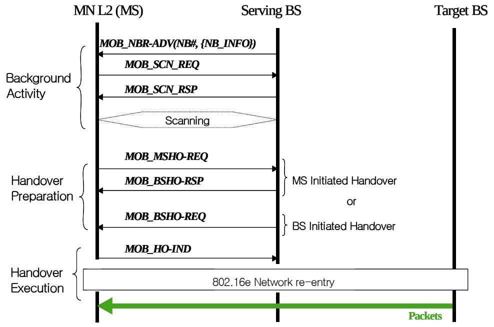


Figure 6. WiBro handoff procedures

3.2 WiBro testbed environments

The WiBro terminal is KWD-U1300 of KT.

The specification of the PC 1 is as follows; OS:Microsoft Windows XP Professional V2002, Service Pack 2, CPU:Intel Core2 6400 2.13Ghz, RAM : 2GB, HDD: 300GB

The specification of the notebook1 is as follows; OS: Microsoft Windows XP Home Edition V2002, Service Pack 2, CPU: Genuine Intel T2400 1.83Ghz, RAM : 1GB, HDD: 30GB

The specification of the notebook2 is as follows; OS: Microsoft Windows XP Professional V2002, Service Pack 3, CPU : Intel pentium 4 2.66GHz, RAM : 448MB, HDD: 160GB

The specification of the notebook 3 is OS:Microsoft Windows XP Professional V2002, Service Pack 2, CPU : Intel ARM 600MHz, RAM: 0.99MB, HDD: 80G

Figure 8. Installing WiBro modem.

3.3 Packet analyzer installing

The packet analyzer is the Cain & Abel. This paper uses the version of v4.49.23 from http://www.oxid.it. The Cain & Abel with WinPcap are installed in the victim and the attacker.

The Wireshark v1.0.4 is also used for packet analysis. it can be downloaded from http://www.wireshark.org. The Wireshark with WinPcap are installed in the victim and the attacker. And e-Watch Lite is used for packet analysis from http://ewatch.hangkong.ac.kr.

3.4 DoS attack tools

HGod.Exe is the DoS attack tool which Chinese hacker Lion developed. It carries out all kinds of Flooding attacks to a windows machine. It can designate the arbitrary source address and the port address in order to spoof the source. And It can generate a large volume of traffic. If the source address is not designated, it is configured randomly so that the address generated randomly could be non-existent address.

TCP/UDP SYN Flooding, ICMP Flooding, IGMP Flooding and DRDoS can be applied to the attack. jolt2.exe is the famous IP fragment attack tool and uses ICMP and UDP protocol.

3.5 DoS attacks

TCP SYN Flooding/DRDoS: the attack generates 100 threads. If the attack is configured by not using IP spoofing, 10 threads generate 145,153 sessions to attack the victim.

ICMP/IGMP Flooding : this attack transmits ICMP echo request/igmp-0 messages. it uses the source spoofing.

ICMP Flooding is able to be recognized by detecting Bad ICMP echo request packets. IGMP Flooding detection is impossible.

IP fragment attack uses ICMP and UDP protocol. While arriving at the victim, the packets should be reconstructed. However, since the attack modifies the offset field and the more fragment field, the packet reconstruction is failed and the victim's system resource is exhausted.

As shown below, malicious packets are used for the attack.
@ ip_off = 65520(fragment offset, 1FFE)
@ ip_id=0x0455 (identification)
@ ip_sum=0xe32e(valid value for avoiding a drop due to checksum)
@ ip_len=29(Total Length, 0x1d)
@ ip_mf=0(configured like last fragment)

4. Packet analysis against DoS attack on WiBro environments

In the experiment, WiBro notebook1 launches DoS attack to PC1, WiBro notebook2 and WiBro notebook3. The packets from WiBro DoS attack are analyzed. And the forensic data are generated. Then traceback is performed.

In order to analyze packets, the Cain & Abel v4.0.23, the Wireshark v1.0.4 and e-Watch Lite are installed in the victim's system.

The test uses 0018 GCT WIBRO USB Network Device and analyzes the packets with WinPcap promiscuous mode. The WiBro mobile terminal is KWD-U1300 released from KT. The specification of the PC 1 is as follows; OS:Microsoft Windows XP Professional V2002, Service Pack 2, CPU:Intel Core2 6400 2.13Ghz, RAM : 2GB, HDD: 300GB The specification of the notebook 1 is as follows; OS: Microsoft Windows XP Home Edition V2002, Service Pack 2, CPU : Genuine Intel T2400 1.83Ghz, RAM : 1GB, HDD: 30GB The specification of the notebook 2 is as follows; OS: Microsoft Windows XP Professional V2002, Service Pack 3, CPU : Intel pentium 4 2.66GHz, RAM : 448MB, HDD: 160GB The specification of the notebook 3 is OS:Microsoft Windows XP Professional V2002, Service Pack 2, CPU : Intel ARM 600MHz, RAM: 0.99MB, HDD: 80G

4.1 Analysis of DoS attack

In the TCP SYN Flooding/DRDoS attack, 10 threads cause the victim to be saturated by 145,153 sessions. The victim's system is down. In the Fragment Attack where the size of each packet is 80KB, one minute later, the victim's system is so slow that valid log-in cannot be processed due to resource exhaustion. The victim's system became crashed soon after. while moving, the victim's system became suspended more early.

In the ICMP/IGMP Flooding attack, a large number of ICMP echo request/igmp-0 messages with the spoofed source address are transmitted. By discovering bad ICMP echo request packets, ICMP flooding attack could be detected. The IGMP Flooding attack was not able to be detected. During attack, the victim's CPU consumed approximately 70% CPU resource. The packets are dropped at the level of the victim's kernel. And there are no logs on the system.

4.2 Analysis of DoS attack packets

In the experiment of WiBro DoS attack, as shown in Figure9, this paper captures packets by using Wireshark and analyzes packets. The analyzed packets with auditing records collected from a audit system are useful to traceback the irregal DoS attack on a network.

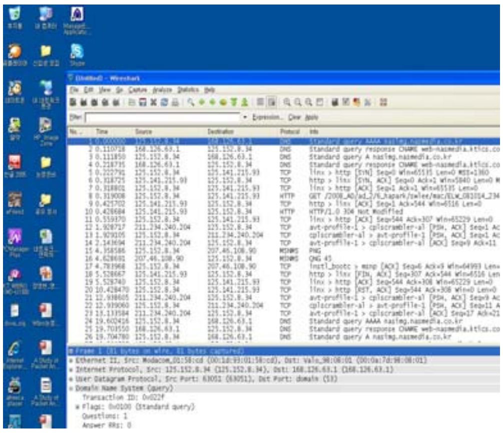
4.2.1 Analysis of DNS packets

at the time 0.000000, Source 125.152.8.34 sends DNS Standard query for resolving AAAA cyad.nate.com to Destination 168.126.63.1.

4.2.2 Analysis of TCP packets

at the Time 0.256863, Source 125.152.8.34 sends a 'TCP ap1x > http [SYN] Seq=0 Win=65535 Len=0 MSS=1360' message to Destination 203.226.255.11.

the destination responded the message by '[SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460'


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply

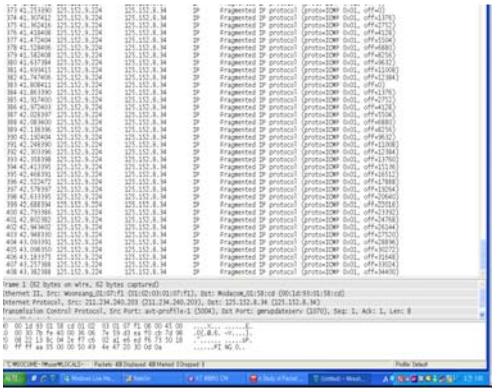
```
No. Time       Source          Destination     Protocol Info
 1 0.000000    125.152.8.34    168.126.63.1    DNS    Standard query AAAA nasimg.nasmedia.co.kr
 2 0.110718    168.126.63.1    125.152.8.34    DNS    Standard query response CNAME web-nasmedia.ktics.co
 3 0.111850    125.152.8.34    168.126.63.1    DNS    Standard query A nasimg.nasmedia.co.kr
 4 0.218735    168.126.63.1    125.152.8.34    DNS    Standard query response CNAME web-nasmedia.ktics.co
 5 0.222791    125.152.8.34    125.141.215.93  TCP    1linx > http [SYN] Seq=0 Win=65535 Len=0 MSS=1360
 6 0.318725    125.141.215.93  125.152.8.34    TCP    http > 1linx [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 M
 7 0.318801    125.152.8.34    125.141.215.93  TCP    1linx > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
 8 0.319008    125.152.8.34    125.141.215.93  HTTP   GET /2008_AD/ad_2/6_hapark/swlee/mac/ELW_081014_234
 9 0.425702    125.141.215.93  125.152.8.34    TCP    http > 1linx [ACK] Seq=1 Ack=544 Win=6516 Len=0
10 0.428684    125.141.215.93  125.152.8.34    HTTP   HTTP/1.0 304 Not Modified
11 0.559370    125.152.8.34    125.141.215.93  TCP    1linx > http [ACK] Seq=544 Ack=307 Win=65229 Len=0
12 1.928717    211.234.240.204 125.152.8.34    TCP    avt-profile-1 > cplscrambler-al [PSH, ACK] Seq=1 Ac
13 1.929105    125.152.8.34    211.234.240.204 TCP    cplscrambler-al > avt-profile-1 [PSH, ACK] Seq=1 Ac
14 2.143694    211.234.240.204 125.152.8.34    TCP    avt-profile-1 > cplscrambler-al [ACK] Seq=9 Ack=11
15 4.358586    125.152.8.34    207.46.108.90   MSNMS  PNG
16 4.628691    207.46.108.90   125.152.8.34    MSNMS  QNG 45
17 4.783968    125.152.8.34    207.46.108.90   TCP    instl_bootc > msnp [ACK] Seq=6 Ack=9 Win=64993 Len=
18 5.528667    125.141.215.93  125.152.8.34    TCP    http > 1linx [FIN, ACK] Seq=307 Ack=544 Win=6516 Len
19 5.528740    125.152.8.34    125.141.215.93  TCP    1linx > http [ACK] Seq=544 Ack=308 Win=65229 Len=0
20 10.428470   125.152.8.34    125.141.215.93  TCP    1linx > http [RST, ACK] Seq=544 Ack=308 Win=0 Len=0
21 12.938605   211.234.240.204 125.152.8.34    TCP    avt-profile-1 > cplscrambler-al [PSH, ACK] Seq=9 Ac
22 12.939060   125.152.8.34    211.234.240.204 TCP    cplscrambler-al > avt-profile-1 [PSH, ACK] Seq=11 A
23 13.133584   211.234.240.204 125.152.8.34    TCP    avt-profile-1 > cplscrambler-al [ACK] Seq=17 Ack=21
24 19.602416   125.152.8.34    168.126.63.1    DNS    Standard query AAAA nasimg.nasmedia.co.kr
25 19.703550   168.126.63.1    125.152.8.34    DNS    Standard query response CNAME web-nasmedia.ktics.co
26 19.704780   125.152.8.34    168.126.63.1    DNS    Standard query A nasimg.nasmedia.co.kr

⊞ Frame 1 (81 bytes on wire, 81 bytes captured)
⊞ Ethernet II, Src: Modacom_01:58:cd (00:1d:93:01:58:cd), Dst: Valo_98:08:01 (00:0a:7d:98:08:01)
⊞ Internet Protocol, Src: 125.152.8.34 (125.152.8.34), Dst: 168.126.63.1 (168.126.63.1)
⊞ User Datagram Protocol, Src Port: 63051 (63051), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x022f
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
```

Figure 9. Packets captured from the victim.

4.2.3 Analysis of HTTP packets

At the Time 0.350500, Source 125.152.8.34 sends a ' GET /js.kti/nateon/nateon.nate.com@s_b_Bottem?age=49&gender=1 http' message



```
373 41.253390 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=0)
374 41.307412 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=1376)
375 41.362416 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=2752)
376 41.418408 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=4128)
377 41.472404 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=5504)
378 41.528406 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=6880)
379 41.582408 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=8256)
380 41.637384 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=9632)
381 41.693413 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=11008)
382 41.747406 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=12384)
383 41.808411 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=0)
384 41.863390 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=1376)
385 41.917400 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=2752)
386 41.972403 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=4128)
387 42.028397 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=5504)
388 42.083400 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=6880)
389 42.138396 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=8256)
390 42.192404 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=9632)
391 42.248390 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=11008)
392 42.303396 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=12384)
393 42.358398 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=13760)
394 42.413395 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=15136)
395 42.468391 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=16512)
396 42.523472 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=17888)
397 42.578397 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=19264)
398 42.633395 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=20640)
399 42.688394 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=22016)
400 42.793386 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=23392)
401 42.802382 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=24768)
402 42.943402 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=26144)
403 42.948330 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=27520)
404 43.093391 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=28896)
405 43.098350 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=30272)
406 43.183375 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=31648)
407 43.257388 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=33024)
408 43.382388 125.152.9.224  125.152.8.34  IP  Fragmented IP protocol (proto=ICMP 0x01, off=34400)

Frame 1 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Woonsang_01:07:f1 (01:02:03:01:07:f1), Dst: Modacom_01:58:cd (00:1d:93:01:58:cd)
Internet Protocol, Src: 211.234.240.203 (211.234.240.203), Dst: 125.152.8.34 (125.152.8.34)
Transmission Control Protocol, Src Port: avt-profile-1 (5004), Dst Port: genupdateserv (1070), Seq: 1, Ack: 1, Len: 8

0  00 1d 93 01 58 cd 01 02  03 01 07 f1 08 00 45 00   ....X... ......E.
0  00 30 7b fe 40 00 36 06  7e 59 d3 ea f0 cb 7d 98   .0{.@.6. ~Y....}.
0  08 22 13 8c 04 2e f7 c6  02 a1 e6 ed f6 71 50 18   .".......  ...qP.
0  ff ff aa 55 00 00 50 49  4e 47 20 30 0d 0a         ...U..PI NG 0..
```

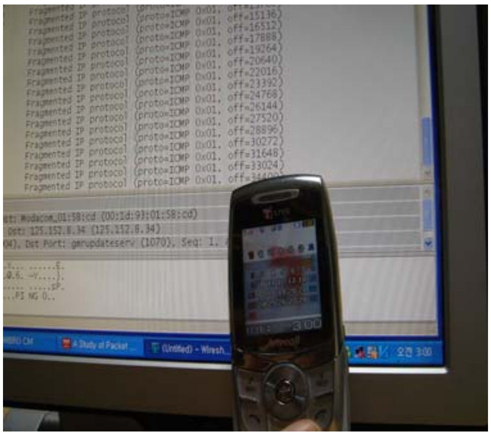
Figure 10. Packets of IP fragmented DoS attack

4.2.4 Analysis of IP fragmented attack packets

As shown Figure 10, at the time 41.253390, the source 125.152.8,34 sends fragmented IP segments (proto=icmp 0x01, off=0) to the destination 125.152.8.34 in order to launce DoS attack.

4.3 Packet analysis and integrity of forensic data

Currently all WCDMA cellular phones conform to standard time in south Korea. Therefore, if the time extracted from the DoS attack packets and the current time from a cellular phone are the same, it can be used to prove the integrity which certifies that the contents of the DoS attack packets are not modified. It can be used the evidence for judging legal responsibility against the DoS attack.



```
Fragmented IP protocol (proto=ICMP 0x01, off=15136)
Fragmented IP protocol (proto=ICMP 0x01, off=16512)
Fragmented IP protocol (proto=ICMP 0x01, off=17888)
Fragmented IP protocol (proto=ICMP 0x01, off=19264)
Fragmented IP protocol (proto=ICMP 0x01, off=20640)
Fragmented IP protocol (proto=ICMP 0x01, off=22016)
Fragmented IP protocol (proto=ICMP 0x01, off=23392)
Fragmented IP protocol (proto=ICMP 0x01, off=24768)
Fragmented IP protocol (proto=ICMP 0x01, off=26144)
Fragmented IP protocol (proto=ICMP 0x01, off=27520)
Fragmented IP protocol (proto=ICMP 0x01, off=28896)
Fragmented IP protocol (proto=ICMP 0x01, off=30272)
Fragmented IP protocol (proto=ICMP 0x01, off=31648)
Fragmented IP protocol (proto=ICMP 0x01, off=33024)
Fragmented IP protocol (proto=ICMP 0x01,

st: Modacom_01:58:cd (00:1d:93:01:58:cd)
 Dst: 125.152.8.34 (125.152.8.34)
4), Dst Port: gmrupdateserv (1070), Seq: 1,
```

Figure 11. Integrity of forensic data

5. Conclusion

This paper analyzes the DoS attack traffic on the WiBro network, generates logs and tracebacks the attacker.

With attaining the integrity against the packets resulted from the malicious DoS attack, the paper provides the framework to generating forensic data.

In the WiBro network environment, the attacker and the victim are the WiBro mobile terminal.

The packet analyzers(Cain & Abel, Wireshark and e-Watch Lite) are installed. The DoS attacks are simulated by using hGod.exe and DoS 5.5.

And the paper analyzes the protocols(DNS, TCP, HTTP, IP, ICMP).

By showing that the time extracted from the DoS attack packets and the time from a cellular phone are the same, the integrity is proved.

The correspondence can be used the evidence for judging legal responsibility against the DoS attack.

When security accidents occur, the forensic data and the traceback data are generated. It fortifies entire WiBro network security.

Future researches require real-time forensic generation and real-time traceback on WiBro IPv6.

References

[1] Jone Bellardo, Stefan Savage, "802.11 Denail-of Service Attacks: real vulnerabilities and practical solution", Usenix Security Symposium, 2003.

[2] M.Bernaschi, F. Ferreri, L. Valcamonnici, "Access point vulnerabilities to DoS attack in 802.11 network"' Wireless Network, 9 October 2006.

[3]Tim Grance, Suznne Chvalier, Karen Kent, Hung Dang, "Guide to Computer and network Data Analysis: Applying Forensic techniques to incident response," NIST, August 2005.

[4] Mark Reith, Clint Carr, Gregg Gunsch, "An Examination of Digital Forensic Model", International Journal of Digital Evidence, 1(3), 2002.

[5] Orin S. Kerr, "Digital Evidence and the New criminal procedure"' Columbia Law review, Vol.105. 2005.

[6] Philip Turner, 'Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags", Digital Investigation 4, pp.30-35, 2007.

[7] IEEE 802.16e, http://standards.ieee.org/getieee802/download/802.16e-2005.pdf

[8] Bsing, M. E., Null. J., & Fprcht, K, "computer forensic ; The modern crime fighting tool"' journal of Computer information System, 46(2), 115-119. 2005.

[9] Ieong R. S. C. "Freeware Live Forensic tools evaluation and operation tips"' 4th Australian Digital Forensic Conference, 2006.

[10] Kanellis, P., Kiountouzis, E., Kolotronis, N., Marrakos, D. (Eds.), "Digital crime and forensic science in cyberspace", Journal of digital forensic practice. Hershey: Idea Group. 2006.

[11] Williamson, B, "Forensic Analysis of the Contents of Nokia Mobile Phones", School of Computer and Information Science Edith Cowan University Perth, 2005.

[12] D. Schnackenberg, K. Djahandary, and D Strene, “Cooperative Intrusion Traceback and Response Architecture(CITRA),”Proceedings of the 2nd DARPA Information Survivability Conference and Exposition(DISCEXII), June 2001.

Biography:

Deawoo Park is an Adjunct Professor of IT Application Science Department at the Hoseo Graduate School of VENTURE, South Korea. Dr. Park received the B.S. degree in computer science from the Soongsil University in 1995. And he received the M.S. degree in 1998. He received the Ph.D. degree from the computer science department of the Soongsil University in 2004. Dr. Park has worked as the Head of Researcher and Developer Laboratories at Magiccastle co., LTD. His interests include Information Security of computer and networks, Ubiquitous Computing, Web Programming, Mobile Communication, Cyber Reality.