# A System for Detecting a Port Scanner in 3G WCDMA Mobile Networks

**K. Sekwon**[1]**, O. Joohyung**[1]**, I. Chaetae**[1]**, and K. Inho**[2]
[1]Korea Internet & Security Agency, IT Venture Tower, Jungdaero 135, Songpa, Seoul 138-950, Korea
[2]SKtelecom, SK T-Tower, 11, Euljiro 2-ga, Jung-gu, Seoul 100-999, Korea

**Abstract** - *Currently, there has been a 3G mobile networks data traffic explosion due to the large increase in the number of smartphone users. Unlike the traditional wired infrastructure, 3G mobile networks have limited wireless resources and signaling procedures for complex wireless resource management. However, mobile network security for various abnormal and malicious traffic technologies was not ready. So malicious or potentially malicious traffic originating from mobile malware infected smart devices can cause serious problems to the 3G mobile networks, such as DoS and scanning attacks in wired networks. In this paper, we describe the port scanning attacks and propose a port scanning detection system based on the Threshold Random Walk (TRW) algorithm in 3G mobile networks. In 3G WCDMA mobile networks, the proposed system detects a variety of port scanning attack in real time. The results of applying the 3G WCDMA mobile network show that the proposed systems are practical and effective.*

**Keywords:** 3G, WCDMA, Port Scanner, TRW

## 1 Introduction

Currently, 3G mobile networks such as WCDMA and CDMA 2000 have been built. As of December 2005, there were over 300 million CDMA subscribers worldwide. Emerging 3G mobile network standards such as EV-DO and HSDPA promise to deliver broadband mobile internet services with peak rates of 2.4 Mbps and 14.4 Mbps, and HSPA+ will allow uplink speeds of 11Mbps and downlink speeds of 42Mbps, respectively. Also 3G mobile networks with a higher mobility than a Wi-Fi environment was provided.

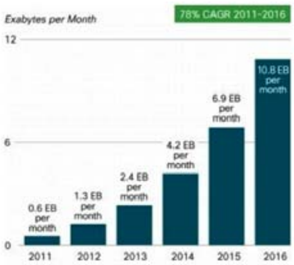


Fig. 1. Cisco Forecasts 10.8 exabytes per month of mobile data traffic by 2016.

However, there has been a 3G mobile network data traffic explosion due to the large increase in the number of smartphone users. Also, new mobile services to satisfy the various needs of smartphone users are being developed day by day. In other words, this means an increase in data traffic over the mobile networks. Fig. 1 shows the mobile data traffic growth forecast[1][2].

Unlike a traditional wired infrastructure, 3G mobile networks have limited wireless resources and signaling procedures for complex wireless resource management. So this data traffic is not a problem in wired networks, but in mobile networks this can be a threat.

Especially, not all of the data traffic that flows into the mobile network is normal. There are segments of unnecessary or abnormal traffic. In the existing wired network, this was not a serious problem, but it can be a threat for the mobile networks, which has a narrow bandwidth and limited wireless resources. In practice, the speed for the data service of 3G mobile networks within crowded locations of smartphone users apparently decreases, or the data service cannot be properly provided[3].

Malicious or potentially malicious traffic originating from mobile malware infected smart devices can cause serious problems to the 3G mobile networks, such as a DoS and scanning attack in wired networks. Unlike the traditional wired network, mobile network security for various abnormal and malicious traffic technologies was not ready. Mobile networks, such as a communication facility, can be viewed as a national infrastructure. If mobile networks are not supported by appropriate security technologies, they can be a target of cyber terrorism by hackers, which can cause serious economic and social losses to mobile communication service providers.

In this paper, we describe port scanning attacks and propose a port scanning detection system based on the Threshold Random Walk (TRW) algorithm in 3G mobile networks[4][5]. And the test results of proposed system is presented in the 3G WCDMA mobile network. This paper is structured as follows: first, in Section 2, we overview the 3G WCDMA mobile networks and TRW algorithm for detecting the port scanner. In Section 3, the port scanning attacks on

3G WCDMA mobile networks are described. In Section 4, we propose the port scanner detection system based on the TRW algorithm. In Section 5, the test results of the proposed systems is presented in the 3G WCDMA mobile network. Finally, conclusions and future works are given in Section 6 and 7.

# 2 Background Information

In this section, we overview the 3G mobile networks and TRW algorithm that can detect a port scanner.

## 2.1 3G WCDMA Wireless Networks

The 3G mobile network technology described in this paper is the WCDMA, which has been adapted as the 3G mobile network technology in many countries. The network structure of the WCDMA is mainly separated by UE, UTRAN, and the Core Network (CN), as Fig. 2.

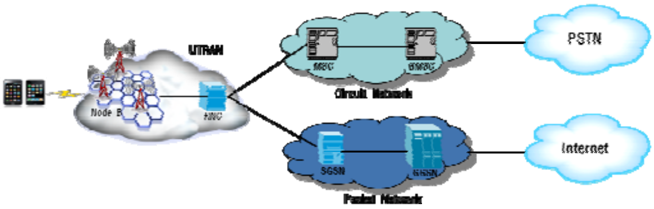


Fig. 2. 3G WCDMA mobile networks.

User Equipment (UE) means a terminal of users that are connected to the 3G mobile network, and UTRAN is a network that controls the wireless resources of terminals. The Core Network can be sub-divided into the Circuit Switched Network for call service and the Packet Switched Network for data service.

The main devices of data transmission over the packet network are the Serving GRPS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). The SGSN is in charge of the service management over the packet network, which is for data service. The GGSN manages IP allocation to terminals and converts the data from the packet network to IP packets to support communications with other Internet networks. Typically, there are multiple SGSNs, each of which serves the GPRS users that are physically located in its serving area.

Another key component of a 3G mobile network is the Radio Network Controller (RNC), which is the point where the wireless link layer protocols terminate. The RNC manages the radio resources for radio access. The RNC provides the interface between a mobile that is communicating through a NodeB and the network edge. This includes the management of radio transceivers in NodeB, admission control, channel allocation, and management tasks such as handoffs between NodeBs, and deciding on the power control parameters. The functionalities of a NodeB include wireless link transmission/reception, modulation/ demodulation, physical channel coding, error handling, and power control.

In this hierarchical architecture, multiple mobiles communicate with a NodeB, multiple NodeBs communicate with an RNC, and multiple RNCs talk to the SGSN/GGSN. Each device uses a different protocol and tunneling. Between the RNC and SGSN is the "Iu-PS" interface, which is usually used in an ATM (Asynchronous Transfer Mode) network. The SGSN and GGSN use a protocol called the GPRS Tunneling Protocol (GTP) to transmit user data and the interface is known as the Gn interface[6]. GTP can be categorized as GTP-U for the packet data, GTP-C for signaling, and GTP (prime) for billing[7]. Fig. 3 shows a 3G WCDMA protocol stack.

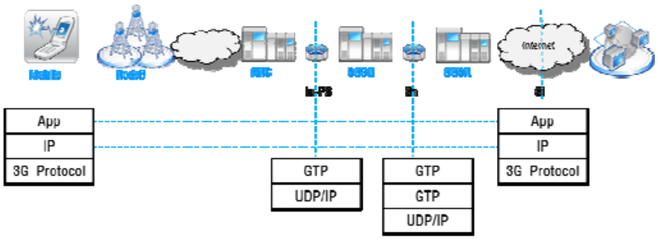


Fig. 3. 3G WCDMA protocol stack.

The UE is representative of smartphones but recently it also includes a variety of devices like laptops and tablets. In particular, a variety of UEs that do not have the function for 3G mobile communication but that have the function for Wi-Fi communication can communicate via 3G mobile networks by using the tethering feature of a smartphone.

The incoming traffic through 3G mobile networks are not only from smartphones but are also from multiple devices such as notebooks and netbooks. Thus, the traffic (in mobile network) will now be observed in various forms.

## 2.2 Related Works

Recently, there is increasing concern about the management and security of 3G mobile networks due to an increase in data traffic that flows into it. Here, not all of the data traffic that flows into the mobile networks is normal[3]. Many detection and corresponding technologies against anomaly traffic in 3G WCDMA mobile networks have been proposed.

F. Ricciato defined anomaly traffic, which might occur in 3G mobile networks, such as scanning or flooding traffic[8]. And V. Falletta tested the syncount and TRW algorithm that can detect port scanners in 3G networks[4].

The TRW algorithm considers two hypothesis, $H_0$ and $H_1$, where $H_0$ is the hypothesis that the given remote source is benign and $H_1$ is the hypothesis that the remote source is a scanner. It also assumes that, conditional on the hypothesis

$H_j$, the random variables $Y_i \mid H_j$, $i = 1, 2, \ldots$ are independent and identically distributed. The distribution of the Bernoulli random variable $Y_i$ can then be expressed as:

$$\begin{aligned} &\Pr[Y_i = 0 \mid H_0] = 0.8, \quad \Pr[Y_i = 1 \mid H_0] = 0.2 \\ &\Pr[Y_i = 0 \mid H_1] = 0.2, \quad \Pr[Y_i = 1 \mid H_1] = 0.8 \end{aligned} \qquad (1)$$

where $Y_i$ is a random variable that represents the outcome of the first connection attempt by remote source to the *i-th* distinct local host.

$$Y_i = \begin{cases} 0 & \text{Connection Success} \\ 1 & \text{Connection Failure} \end{cases} \qquad (2)$$

And, it calculates the likelihood ratio $\Lambda(Y)$ as follows:

$$\Lambda(Y) = \frac{\Pr[Y \mid H_1]}{\Pr[Y \mid H_0]} = \prod_{i=1}^{n} \frac{\Pr[Y_i \mid H_1]}{\Pr[Y_i \mid H_0]} \qquad (3)$$

Finally, the likelihood ratio is compared to an upper threshold, $\eta_1$, and a lower threshold, $\eta_0$. If $Y_i$ then a remote source is a scanner. If $\Lambda(Y) \geq \eta_1$ then a remote source is benign. And if $\eta_0 < \Lambda(Y) < \eta_1$ then it waits for the next observation and updates $\Lambda(Y)$. Fig. 4 shows the flow diagram of the TRW algorithm that can detect a port scanner.

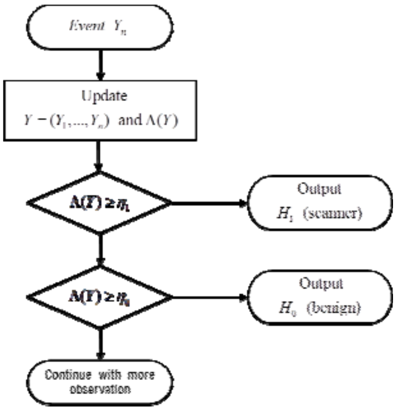


Fig. 4. The flow diagram of TRW algorithm.

# 3 Port Scanning Attack

Scanning attacks are performed to find out the network architecture or the network vulnerability of any systems. It causes a high volume of traffic because of sending traffic to multiple systems at a remote site. Scanning traffic over a general wired-network cannot be a serious problem. In the 3G WCDMA mobile network, however, the problem shows a different aspect. Most of the scanning traffic causes paging traffic and it makes traffic volume weighted in the 3G WCDMA mobile network[3]. In addition, the critical information of 3G WCDMA mobile network configuration equipment, such as the IP address and port number, are exposed by scanning attacks. Therefore, scanning attacks are more fragile than a wired network at the 3G WCDMA wireless network, because it is a closed type of service structure and has a narrow bandwidth and limited wireless resource.

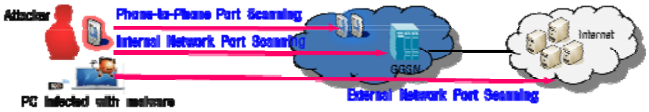
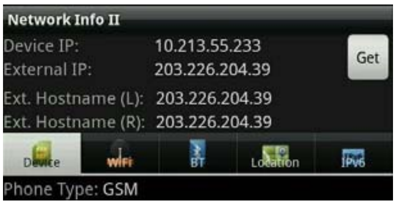

Attacker
Phone-to-Phone Port Scanning
Internal Network Port Scanning
GGSN
Internet
PC Infected with malware
External Network Port Scanning

Fig. 5. Port scanning attacks over 3G WCDMA mobile networks.

Fig. 5 shows port scanning attacks in 3G WCDMA mobile networks. An attacker can do scanning attacks using port scanner applications (Port Scanner, TCP Port Scanner, Net Scan, etc.) or tools (Nmap, Superscan, etc.) as follows:

## 3.1 Phone-to-Phone Port Scanning

Check the IP address assigned to the smartphone using applications such as Network Info II



Network Info II

Device IP: 10.213.55.233

External IP: 203.226.204.39

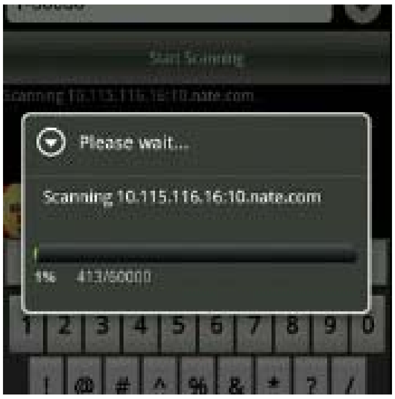
Ext. Hostname (L): 203.226.204.39

Ext. Hostname (R): 203.226.204.39

Phone Type: GSM

Fig. 6. Check IP address assigned to the smart-phone via Network Info II.

Perform a port scanning attack on the target smartphone of the same IP range using the Port Scanner application



Scanning 10.115.116.16:10.nate.com

Please wait...

Scanning 10.115.116.16:10.nate.com

1% 413/60000

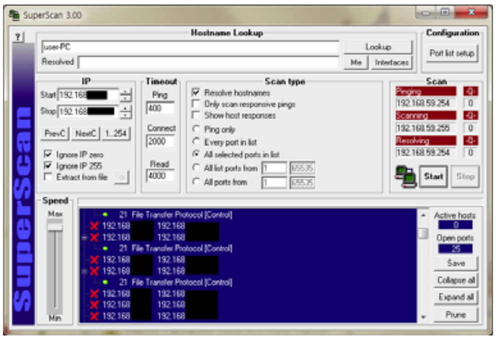
Fig. 7. Port scanning attack on target smart-phone using the Port Scanner application.

## 3.2 Internal Network Port Scanning

Connect a PC to the 3G WCDMA mobile network via the tethering function of the smartphone

Obtain the internal network IP information of the mobile communication service provider via tracert

Perform port scanning attacks on the internal network using the port scanning tool, Superscan



SuperScan 3.00

Hostname Lookup: user-PC

Resolved:

IP
Start 192.168[redacted]
Stop 192.168[redacted]

☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
☑ Resolve hostnames
☐ Only scan responsive pings
☐ Show host responses
○ Ping only
○ Every port in list
● All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535

Scan
Pinging 192.168.59.254 0
Scanning 192.168.59.255 0
Resolving 192.168.59.254 0

```
    21  File Transfer Protocol [Control]
 ✕ 192.168[redacted]  192.168[redacted]
 ✕ 192.168[redacted]  192.168[redacted]
    21  File Transfer Protocol [Control]
 ✕ 192.168[redacted]  192.168[redacted]
 ✕ 192.168[redacted]  192.168[redacted]
    21  File Transfer Protocol [Control]
 ✕ 192.168[redacted]  192.168[redacted]
 ✕ 192.168[redacted]  192.168[redacted]
 ✕ 192.168[redacted]  192.168[redacted]
```

Active hosts 0
Open ports 25

Fig. 8. Port scanning attack using Superscan.

## 3.3 External Network Port Scanning

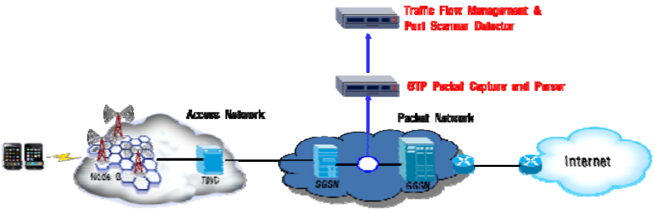
Connect a PC to the 3G WCDMA mobile network via the tethering function of the smartphone

Perform port scanning attacks on the target server in the external network

# 4 System Architecture

In this section, the architecture of the proposed system for port scanner detection in 3G WCDMA networks will be described in detail.

The overall architecture is shown in Fig. 9. It consists of two separate systems, which are the GTP Packet Capture and Parser and the Traffic Flow Management and Port Scanner Detector. The first system captures in/outbound GTP-C packets and outbound GTP-U packet in a Gn interface with an average 6.5Gbps, and extracts the necessary information. The second system consists of the Traffic Flow Management Module that manages the user's session/data flow information and the Port Scanner Detection Module that detects port scanners.



Traffic Flow Management & Port Scanner Detector
GTP Packet Capture and Parser
Access Network
Packet Network
Node B
RNC
SGSN
GGSN
Internet

Fig. 9. The structure of port scanner detection systems.

## 4.1 GTP Packet Capture and Parser

Fig. 10 shows the structure of a GTP Packet Capture and Parser. In this system, the DAG Card based on the data stream capturing technique is applied for capturing GTP packets in real time. It captures mirrored GTP packets in the Gn interface and stores them in the buffer. Then it checks the type of GTP packet messages and extracts the fields of GTP messages depending on the type as shown in Table I. If the GTP packet is outbound GTP-U, the GTP Packet Capture and Parser discards the packet.

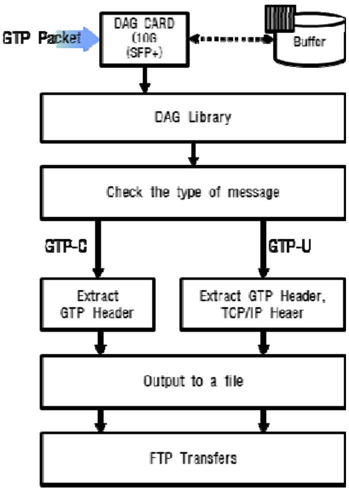
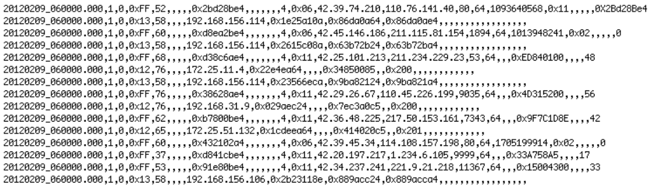


Fig. 10. The structure of GTP Packet Capture and Parser.

TABLE I. THE EXTRACTION FIELD OF GTP MESSAGE IN ACCORDING TO THE TYPE OF MESSAGE

| Type of Message | | GTP Header | GTP Ext Header | TCP(UDP)/IP Header |
|---|---|---|---|---|
| GTP-C | Create request (0x10) | Protocol Type, Reserved, Message Type, Total Length, | IMSI, APN, MSISDN, GSN, TEID, Downlink TEID(Ctl), Downlink TEID(Data) | |
| | Create response (0x11) | | GSN, TEID, Upnlink TEID(Ctl), Uplink TEID(Data), End user Address | |
| | Update request (0x12) | | GSN, TEID, Downlink TEID(Data) | |
| | Update response (0x13) | | GSN, TEID, Upnlink TEID(Ctl), Uplink TEID(Data) | |
| | Delete request (0x14) | | TEID | |
| | Delete response (0x15) | | | |
| GTP-U (0xFF) | | | TEID | Version, Protocol, Source IP, Dest IP, Dest Port, TTL, Sequence Num, Control Bit |

The output is saved as a file, as shown in Fig. 11. Then, the output file is transmitted to the Traffic Flow Management & Port Scanner Detection via FTP every 1 minute.

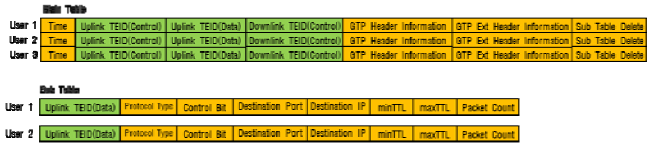


```
20120209_060000.000,1,0,0xFF,52,,,,,0x2bd28be4,,,,,,,4,0x06,42.39.74.210,110.76.141.40,80,64,1093640568,0x11,,,,,0X2Bd28Be4
20120209_060000.000,1,0,0x13,58,,,,192.168.156.114,0x1e25a10a,0x86da0a64,0x86da0ae4,,,,,,,,,,,,,,,,
20120209_060000.000,1,0,0xFF,60,,,,,0xd8ea2be4,,,,,,,4,0x06,42.45.146.186,211.115.81.154,1894,64,1013948241,0x02,,,,,0
20120209_060000.000,1,0,0x13,58,,,,192.168.156.114,0x2615c08a,0x63b72b24,0x63b72ba4,,,,,,,,,,,,,,,,
20120209_060000.000,1,0,0xFF,68,,,,,0xd38c6ae4,,,,,,,4,0x11,42.25.101.213,211.234.229.23,53,64,,,0xED840100,,,,48
20120209_060000.000,1,0,0x12,76,,,,172.25.11.4,0x22e4ea64,,,,0x34850085,,0x200,,,,,,,,,,,,
20120209_060000.000,1,0,0x13,58,,,,192.168.156.114,0x23566eca,0x9ba82124,0x9ba821a4,,,,,,,,,,,,,,,,
20120209_060000.000,1,0,0xFF,76,,,,,0x38628ae4,,,,,,,4,0x11,42.29.26.67,110.45.226.199,9035,64,,,0x4D315200,,,,56
20120209_060000.000,1,0,0x12,76,,,,192.168.31.9,0x029aec24,,,,0x7ec3a0c5,,0x200,,,,,,,,,,,,
20120209_060000.000,1,0,0xFF,62,,,,,0xb7800be4,,,,,,,4,0x11,42.36.48.225,217.50.153.161,7343,64,,,0x9F7C1D8E,,,,42
20120209_060000.000,1,0,0x12,65,,,,172.25.51.132,0x1cdeea64,,,,0x414020c5,,0x201,,,,,,,,,,,,
20120209_060000.000,1,0,0xFF,60,,,,,0x432102a4,,,,,,,4,0x06,42.39.45.34,114.108.157.198,80,64,1705199914,0x02,,,,,0
20120209_060000.000,1,0,0xFF,37,,,,,0xd841cbe4,,,,,,,4,0x11,42.20.197.217,1.234.6.105,9999,64,,,0x33A758A5,,,,17
20120209_060000.000,1,0,0xFF,53,,,,,0x91e80be4,,,,,,,4,0x11,42.34.237.241,221.9.21.218,11367,64,,,0x15004300,,,,33
20120209_060000.000,1,0,0x13,58,,,,192.168.156.106,0x2b23118e,0x889acc24,0x889acca4,,,,,,,,,,,,,,,,
```

Fig. 11. The output of GTP Packet Capture and Parser.

## 4.2 Traffic Flow Management

In WCDMA mobile networks, all of the users are assigned unique control and data tunnel endpoint identifier (TEID), respectively, through which the control and data messages are sent and received. Information, such as MSISDN, IMSI, and IP, which could identify users, does not exist in all of the GTP messages. Therefore, it is necessary for user-specific traffic information extraction to manage the TEID contained in a GTP message. In this paper, control and data traffic flow are managed based on the TEID through the analysis of GTP messages.



Main Table

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| User 1 | Time | Uplink TEID(Control) | Uplink TEID(Data) | Downlink TEID(Control) | GTP Header Information | GTP Ext Header Information | Sub Table Delete |
| User 2 | Time | Uplink TEID(Control) | Uplink TEID(Data) | Downlink TEID(Control) | GTP Header Information | GTP Ext Header Information | Sub Table Delete |
| User 3 | Time | Uplink TEID(Control) | Uplink TEID(Data) | Downlink TEID(Control) | GTP Header Information | GTP Ext Header Information | Sub Table Delete |

Sub Table

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| User 1 | Uplink TEID(Data) | Protocol Type | Control Bit | Destination Port | Destination IP | minTTL | maxTTL | Packet Count |
| User 2 | Uplink TEID(Data) | Protocol Type | Control Bit | Destination Port | Destination IP | minTTL | maxTTL | Packet Count |

Fig. 12. The main table and sub table for traffic flow management.

The Traffic Follow Management module consists of a main table and a large sub-table as shown in Fig. 12. Each user's session information, such as TEID, MSISDN, IMSI, and IP address, is managed in the main table, and the transmission information of each user's data traffic, such as Protocol Type, Control Bit, Destination IP, and TTL, is managed in the sub-table. Here, the Uplink Data TEID is used to map the Main Table and Sub-Table.

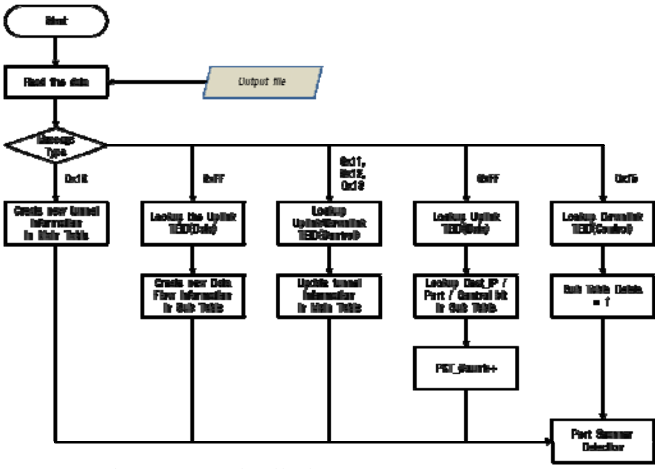

Start
Read the data
Output file
Message Type
0x10
0xFF
0x11,
0x12,
0x13
0xFF
0x15
Create new tunnel information In Main Table
Lookup the Uplink TEID(Data)
Lookup Uplink/Downlink TEID(Control)
Lookup Uplink TEID(Data)
Lookup Downlink TEID(Control)
Create new Data Flow information In Sub Table
Update tunnel information In Main Table
Lookup Dest_IP / Port / Control bit In Sub Table
Sub Table Delete = 1
PKT_Count++
Port Scanner Detection

Fig. 13. The flow diagram of traffic flow management.

Fig. 13 shows the flow diagram of traffic flow management. In the output file received from the GTP Packet Capture and Parser, a new row is added in the main table if the type of message is GTP-C Create Request (0x10) and then the new user's session information is written. If the type of message is GTP-C Creates Response (0x11) or Update Request/Response (0x12/0x13), the user's session information of row with same uplink Control TEID is updated. If the type of message is GTP-C Delete Response (0x15), the Sub Table Delete variable of row with same Download Control TEID is set to 1. Here, Sub Table Delete is a variable used to delete the sub table, and it is changed by Port Scanner Detection that is described in Section 4.3.

When the type of message is same as GTP-U (0xFF), sub table is created if there isn't the sub table of user with same uplink Data TEID or one of destination IP, destination port, Control bit is different, then the user's data transmission information is written. If all of destination IP, destination port, Control bit is same, Packet Count is increased. Once all the packets in the file are analyzed, the Scanner Detection Module is performed. The Port Scanner Detection Module is described below.

## 4.3 Port Scanner Detection

It is limited that a smartphone connects to a large remote source at the same time, and the frequency of repetitive connection attempts is low. Thus, we detected port scanning attacks in case the smartphone fails to connect to multiple IP addresses or to multiple ports of a specific IP address, and the user that caused the port scanning attack is identified based on the traffic flow. In this paper, the TRW algorithm that is described in Section 2 is adopted for detection of the port scanner. In the TRW algorithm, the response to a connection attempt is essential. However, there isn't a response to a connection attempt because the GTP Packet Capture and Parser don't capture inbound GTP-U packets in a Gn interface. So we can't know whether the connection attempt is successful or not. Therefore, we assumed that the connection attempt by a remote source to the distinct local host is successful if the Packet Count is 1, and that it is unsuccessful if the Packet Count isn't 1.

Fig. 14 shows the flow diagram for detecting these port scanning attacks. The marked parts in Fig. 14 are calculated repeatedly until all of the user's data transmission information is analyzed. And, the repeat count is different depending on the Packet Count. Here, $S_n$ is the probability of success for the connection attempt and $F_n$ is the probability of failure regarding the connection attempt. We assume $S_n$ and $F_n$ to be as follows:

$$S_n = 0.8, \quad F_n = 0.2 \tag{4}$$

The likelihood ratio is compared to an upper threshold of $\eta_1$, and a lower threshold of $\eta_0$. We assume $\eta_1$ and $\eta_0$ respectively as follows:

$$\eta_1 = 99, \quad \eta_0 = 0.01 \tag{5}$$

If $\Lambda_n \geq \eta_1$, a remote source is a scanner. If $\Lambda_n \leq \eta_0$, a remote source is benign. Then, the Sub-Table Delete variable is set to 0 and $\Lambda_n$ is initialized to 1. And, if $\eta_0 < \Lambda_n < \eta_1$, the Sub-Table Delete variable is set to 1. It then waits for the next observation and updates $\Lambda_n$. If the Sub-Table Delete variable is 0, all of the user's data transmission information is deleted. If not, it is not deleted for the next observation

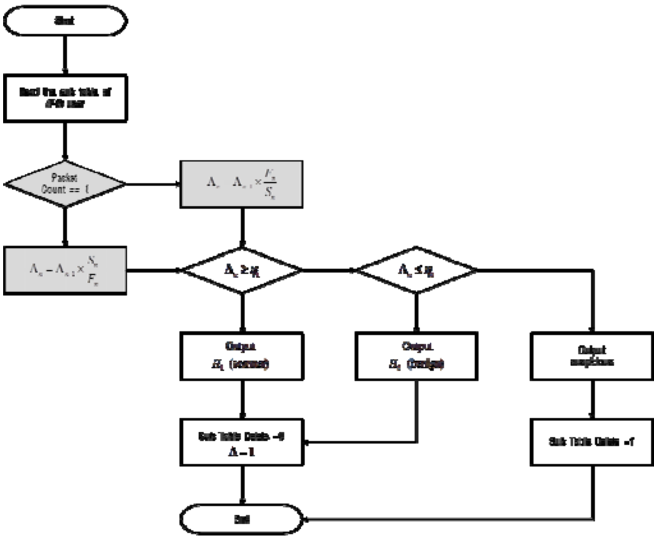


Fig. 14. The flow diagram for detecting port scanning attacks.

## 5 Test Results in 3G WCDMA Networks

The proposed system was tested in the 3G WCDMA mobile network that operates in Korea. Fig. 15 shows the test environment in the 3G WCDMA mobile network. The GTP Packet Capture and Parser system and the Traffic Flow Management and Port Scanner Detection system are installed in the Gn interface of the mobile communication service provider. The input of the GTP Packet Capture and Parser system is the traffic tapping the in/ outbound GTP traffic from one of the GGSNs And the input is the traffic of approximately 2.5 million subscribers with an average of 6.5Gbps. In addition, we performed scanning attacks to evaluate the performance of the proposed systems via tethering. The traffic was incoming to the core of the 3G WCDMA mobile network.

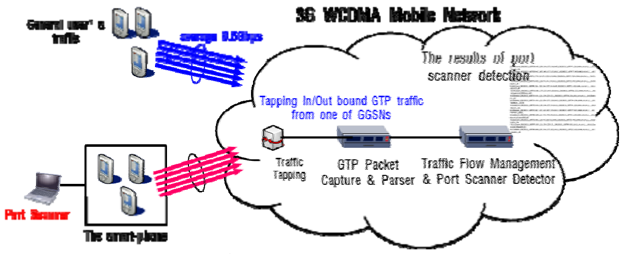

3G WCDMA Mobile Network
General user's traffic
average 6.5Gbps
The results of port scanner detection
Tapping In/Out bound GTP traffic from one of GGSNs
Traffic Tapping
GTP Packet Capture & Parser
Traffic Flow Management & Port Scanner Detector
Port Scanner
The smart-phone

Fig. 15. The test environment for port scanner detection in the 3G WCDMA network.

In test, the GTP Packet Capture and Parser system captured GTP traffic without loss and that the Traffic Flow Management Module managed the user's session/data flow information without delay. And, the Port Scanner Detection Module normally detected all of the scanning traffic caused by us, as shown in Table II.

In Table II, false positive means that the Port Scanner Detection Module misjudges normal user's data traffic with scanning traffic. An example of false positive is traffic to access a particular service like an apple push server (IP address : 17.149.36.71~337, Port : 5223). To prevent a false positive we registered the IP address and port used to access the particular service on a whitelist. The traffic with a registered IP address and port are excluded from port scanning detection.

TABLE II. THE TEST RESULTS OF PORT SCANNER DETECTION MODULE IN 3G WCDMA MOBILE NETWORK

| (A)<br>The number of occurrence of port scanning attack | (B)<br>The number of detection | (C)<br>The number of False positive | (D)<br>The number of additional detection | Results | |
|---|---|---|---|---|---|
| | | | | Detection rate | False positive rate |
| 2,000 | 2,027 | 8 | 19 | 100% | 0.39% |

Here, the detection rate and false positive rate are calculated as follow:

$$Detection\ Rate = \frac{B-(C+D)}{A} \times 100 \tag{6}$$

$$False\ Negative\ Rate = \frac{C}{B} \times 100 \tag{7}$$

We may need to pay attention to the additional detection as (D). It represents the number of scanning attacks among general user's traffic, and the results of the analysis is as follows:

### 5.1 Phone-to-Phone Port Scanning

Through the results of the detection log analysis we found that a smartphone scans over port 22 (ssh) of other smartphones in the same IP range. The IP address of the target smartphone is 42.45.121.7~42.45.121.17. And, the scanning attack is performed in smartphones from the fact that TTL is 64.

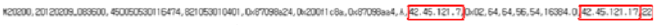
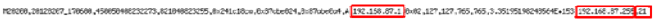

```
K20200,20120209,083600,450050530116474,821053010401,0x87098a24,0x20011c8a,0x87098aa4,4,42.45.121.7,0x02,64,64,56,54,16384,0,42.45.121.17,22
```

Fig. 16. The detection log of phone-to-phone port scanning.

### 5.2 Internal Network Port Scanning

Through the results of the detection log analysis we found that a smartphone scans over port 21 (ftp) of the internal network. And, the scanning attack is performed via tethering from the fact that TTL is 127.

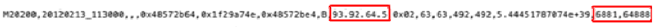


```
M20200,20120207_170600,4500504882232273,8210408823255,0x241c18ce,0x37dbe024,0x87abe6a4,#192.158.87.1 0x02,127,127,765,765,3.3519519024956E+153 192.168.87.255,21
```

Fig. 17. The detection log of phone-to-phone port scanning.

### 5.3 External Network Port Scanning

Through the results of the detection log analysis we found that a smartphone scans over ports 6,881-64,888 of the system in the external network. The IP address of the target system is 93.92.64.5. And the scanning attack is performed via tethering from the fact that TTL is 127.



```
M20200,20120213_113000,,,0x48572b64,0x1f29a74e,0x48572be4,B 93.92.64.5 0x02,63,63,492,492,5.44451787074e+39,6881,64888
```

Fig. 18. The detection log of phone-to-phone port scanning.

## 6 Conclusion

Unlike a traditional wired infrastructure, mobile networks have limited radio resources and signaling procedures for complex radio resource management. So, unwanted traffic is not a problem in wired networks, but for mobile networks it can be a threat. Also, the previous mobile networks seemed to have been relatively safe from external threats because of their close characteristics. However, security threats, which were also in the wired networks, appeared after the switch to the 3G mobile network, and there are practical cases of data service disorders that have been caused by these security threats. Especially, the propagation of smartphones has rapidly expanded and various mobile services appear to be attracting more users, so that security threats to the mobile network have a greater ripple effect.

In this paper, we have proposed systems that are based on the TRW algorithm to effectively detect a port scanner. The proposed systems capture the GTP packet in the Gn interface and manage the user's session/data flow information. The proposed system detects scanning attacks over the multi-port of a target system and one port of IP range. Test results in the 3G WCDMA Network of mobile communication service providers show that the proposed system accurately detect port scanners. Moreover, the proposed system are running on the 3G WCDMA Network, which is operating Korea, without delay.

## 7 Future Work

We captured in/outbound GTP-C and outbound GTP-U packets in the Gn interface and detected port scanners. We will analyze various services that are using specific ports, and improve the accuracy of port scanner detection by capturing inbound GTP-U packets in the Gn interface. Additionally, we will apply the proposed system to the 4G LTE Network of mobile communication service providers that are operating Korea.

## Acknowledgment

This research was supported by the KCC(Korea Communications Commission), Korea, under the R&D program supervised by the KCA(Korea Communications Agency)" (KCA-2012-11912-06001).

## 8 References

[1] Mobile Traffic Data(2011~2016), CISCO VNI Mobile, 2012.

[2] Global Mobile Data Traffic. By Type, Morgan Stanley, 2010.

[3] F. Ricciato, "Unwanted Traffic in 3G Networks," *ACM SIGCOMM Computer Communication Review*, Vol.36, Issue 2, pp. 53-56, April, 2006.

[4] V. Falletta, F. Ricciato, "Detecting Scanners: Empirical Assessment on a 3G Network," *International Journal of Network Security*, Vol.9, No.2, 2009, 143-155.

[5] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing," *Proceedings of the IEEE symposium on Security and Privacy*, pp. 211-225, May, 2004.

[6] H. Holma, A. Toskala, WCDMA for UMTS – Radio Access for third Generation Mobile Communications 3rd, Willey, 2004.

[7] 3GPP, GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 10), TS 29.060 V10.2.0, 2011.

[8] V. Falletta, F Ricciato, P. Romirer-Maierthofer "Traffic Analysis at Short Time-Scales: An Empirical Case Study from a 3G Cellular Network," *IEEE Transactions on Networks and Service Management*, Vol.5, No.1, pp.11-21, March, 2009.