A System for Scanning Traffic Detection in 3G WCDMA Network

Sekwon Kim †, Joohyung Oh and Chaetae Im
Advanced Technology Development Team, Korea Internet & Security Agency, Jungdaero 135, Songpa, Seoul, Korea

Abstract. Recently, with explosion of smart phone users and increasing variety of mobile services, the 3G WCDMA wireless network had been changed to open type service structure from the closed type service structure. In open structure, any device which uses 3G service will be able to access to the wireless network for mobile internet. Also, any data traffic originated from smartphone and tablet would be allowed to access 3G wireless network regardless of whether it is malicious or not. In this situation abnormal traffic, such as scanning attack, may cause serious interference of 3G WCDMA wireless network with the narrow bandwidth and limited wireless resource. However, the existing IP-based traffic analysis and detection techniques are not suitable to apply in the wireless network using application-layer protocol. In this paper, we propose a system for detecting scanner that generates a high volume of traffic in 3G wireless network. The proposed system can detect scanning traffic as quickly well as manage memory efficiently.

Keywords: 3g, wcdma, scanner, bloom filter.

1. Introduction

Third generation (3G) wireless network based on the CDMA2000 and UMTS standards are widely deployed. As of December 2005, there were over 300 million CDMA subscribers worldwide. Emerging 3G data 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, respectively. However, data traffic explosion due to a large increase in the number of smart phone users, widely-spread online application is troubling mobile carriers [1][2]. Especially, abnormal traffic, such as scanning traffic, originated from mobile smart device may cause serious interference of 3G WCDMA wireless network. Scanning attack is performed to find out network vulnerability of any systems and causes a high volume of traffic because of sending traffic to multiple systems at the remote site. At 3G WCDMA wireless network with the narrow bandwidth and limited wireless resource, scanning attack is more fragile than wired network.

In this paper, we propose the architecture of scanning traffic detection system. The proposed system detects scanning traffic through the verification of sequential hypothesis. And it efficiently manages memory using bloom filter. This paper is structured as follows. We present background information related to 3G WCDMA wireless network in Section 2. In section 3, we describe the algorithm of scanning traffic detection and the architecture of system. And we conclude our paper in Section 4.

2. Background Information

In this paper, we propose the architecture of scanning traffic detection system. The proposed system detects scanning traffic through the verification of sequential hypothesis. And it efficiently manages memory using bloom filter. This paper is structured as follows. We present background information related to 3G WCDMA wireless network in Section 2. In section 3, we describe the algorithm of scanning traffic detection and the architecture of system. And we conclude our paper in Section 4.

† Corresponding author. Tel.: + 82-2-405-5422; fax: +82-2-405-5129.
E-mail address: heath82@kisa.or.kr.
2.1. 3G wcdma wireless network

Fig.1 shows the typical architecture of a packet switch network of 3G WCDMA wireless network. We first describe two of its main components: the Gateway GPRS Support Node (GGSN) and the Serving GPRS Support Node (SGSN).

![Packet Switch Network](image)

Fig. 1: Packet switch network of 3G WCDMA wireless network.

The GGSN is a GPRS network entity that serves as the mobile wireless gateway between an SGSN and the Internet. When a mobile successfully authenticates and registers with the network, a Point-to-Point (PPP) link is set up between the GGSN and the mobile. On the other hand, the SGSN is responsible for sending data to and from mobile stations, in addition to maintaining information about the location of a mobile and performing authentication for the mobile. Typically, there are multiple SGSNs, each of which serves the GPRS users physically located in its serving area. Another key component of a UMTS network is the Radio Network Controller (RNC), which is the point where wireless link layer protocols terminate. The RNC provides the interface between a mobile communicating through a Base Station (BS) and the network edge. This includes management of radio transceivers in BS equipment (radio resource control), admission control, channel allocation, as well as management tasks such as handoffs between BSs and deciding power control parameters. The functionalities of a BS include wireless link transmission/reception, modulation/demodulation, physical channel coding, error handling, and power control. In this hierarchical architecture, multiple mobiles communicate with a BS, and multiple BSs communicate with an RNC, and multiple RNCs talk to the SGSN/GGSN.

2.2. Scanner in 3g wcdma wireless network

Scanning attack is 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 the remote site. Also, most of the scanning traffic cause paging traffic, it makes traffic volume weighted at 3G WCDMA wireless network[3]. In addition, the critical information of 3G network configuration equipment, such as ip address, port number, is exposed by scanning attack.

Therefore scanning attack is more fragile than wired network at 3G WCDMA wireless network. Because it is the closed type service structure and has the narrow bandwidth and limited wireless resource.

2.3. Related works

Recently many detection and corresponding technologies against anomaly traffic in 3G WCDMA wireless network had proposed. Ricciato defined an anomaly traffic, which might occur in 3G wireless networks such as scanning or flooding traffic[4]. And Falletta proposed the Threshold Random Walk(TRW) algorithm that can detect scanning traffic[5]. However, TRW algorithm has weakness that is difficult to detect scanning traffic using UDP, ICMP protocol, or if scanning happens repeatedly. Also it didn’t propose the efficient way for processing a high volume of the traffic in real time. And the efficient way of memory management was proposed to processing a high volume of the traffic in real time, but it didn’t consider 3G wireless network in [6].

3. System Architecture
In this section, the architecture of the proposed scanning traffic detection will be described in detail. The overall architecture of the system is shown in Fig. 2. In this system, we have applied hardware based on data stream capture technique to capture network packets in real time.

There are mainly 3 modules in this architecture. GTP Packet Capture and Parser Module captures GTP-U data traffic in Gn and extracts the necessary information such as ip address, control bit, sequence number, etc. Traffic Flow Management Module manages the flow information of in/out-bound data traffic. And Scanning Traffic Detection Module analyzes data traffic and detects abnormal scanning traffic.

![Packet switch network of 3G WCDMA wireless network.](image)

3.1. Scanning traffic detection

We have applied the TRW algorithm to detect scanning traffic. The TRW algorithm assumes the probability of success or failure that attempts to connect to remote local host, and use it to detect scanning traffic.

Fig. 3 shows the algorithm of scanning traffic detection that is adopted TRW. Calculation Condition was set as follows, considering reconnection according to the connection attempt fails.

![The diagram of detection algorithm.](image)
And, we assume the success or failure probability of connection attempt when a remote source is benign($H_0$) or scanner($H_1$), as follows.

\[
\begin{align*}
Pr[Y_i = 0 | H_0] &= 0.8, & Pr[Y_i = 1 | H_0] &= 0.2 \\
Pr[Y_i = 0 | H_1] &= 0.2, & Pr[Y_i = 1 | H_1] &= 0.8
\end{align*}
\]

where $Y_i$ denotes the result that a remote source attempts to connect to $i$-th remote local host.

\[
Y_i = \begin{cases} 
0 & \text{Connection Success} \\
1 & \text{Connection Failure} 
\end{cases}
\]

Finally, we calculate TRW as follows, and detect scanner through comparing to threshold.

\[
TRW = \frac{\Pr[Y_i | H_1]}{\Pr[Y_i | H_0]} = \prod_{i=1}^{n} \frac{\Pr[Y_i | H_1]}{\Pr[Y_i | H_0]}
\]

3.2. The efficient way of memory management

We have applied the Bloom Filter to detect scanning traffic using UDP, ICMP protocol, or repeatedly happened scanning traffic.

Fig.4 shows the efficient way of memory management using the Bloom Filter. We use hashed source IP address as the unique value, record destination IP address in Managing the connection attempt field and Response status management field. Thus, by managing each status information, repetitive input is eliminated, the request message and the response message can be easily mapped. Finally, memory is managed efficiently by removing the memory periodically at the time for managing source IP.

4. Conclusion

The scanning traffic detection is very important to the overall health of 3G WCDMA wireless networks. Since 3G WCDMA wireless network was a closed service structure, there is not much research for 3G network security. In this paper, we have proposed a system for detecting scanning traffic in 3G wireless network. The proposed system can detect scanning traffics quickly well as manage memory efficiently. However, since evaluation is not performed it is not sufficient in many cases. Thus, our future work will focus on implementation of our proposed system for experiment and evaluation of the system design.

5. 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-2011-11914-06001)

6. References