Transmission Time-based Authentication Scheme Using 3G Mobile Device for DRM System

Takahiro Tsuchiya, Masami Kihara
Graduate School of Science and Technology
Nihon University
Funabashi, Japan
tsuchiya.nu@gmail.com

Arjulie John P. Berena
Post-doctoral Fellow
National Institute of Informatics
Tokyo, Japan
ajberena@gmail.com

***Abstract*— The recent widespread deployment of 3G technology has opened the possibility for high value digital content to be delivered to wireless-driven output terminals that may or may not be mobile. This calls for a robust DRM (Digital Rights Management) system that can protect copyrighted content from being illegally accessed. The conventional method of authenticating a registered user or a prospective content purchaser is by means of the username and password combination. However, this method raises many vulnerabilities, especially now that password attacks and phishing techniques are rampant. Enhanced user authentication schemes are thus needed to ensure that the content is delivered to the legitimate purchaser, and to combat piracy in the Internet in general. Our assumed DRM system utilizes 3G mobile devices, such as HSDPA (High Speed Downlink Packet Access) enabled mobile devices, to access the content. An essential part of the system is an access area restriction scheme; it is based on the physical location of the user's mobile device as estimated from the packet transmission time between the mobile device and the server. Together with personal information, the access location must be pre-registered to realize location-specific enforcement policies. This system is extremely flexible and supports a wide range of security policies; for example, the content provider can stipulate that service is terminated if the registered user moves away from the registered terminal through which he is accessing the content.**

I. INTRODUCTION

3G services have been offered by W-CDMA (Wideband Code Division Multiple Access) method systems since 2001 in Japan. The number of users began to rapidly increase from about 2003 because of the emergence of new services, the improvement in the functionality and performance of the mobile devices, and the expansion of the service areas. The international adoption of Wideband Code Division Multiple Access is also advancing smoothly. There were few mobile network operators in 2003, but many new operators have emerged since then. In the countries other than Japan the W-CDMA scheme is called UMTS (Universal Mobile Telecommunications System) or 3G. Recent new services such as the sending and receiving of animated content, online music distribution and the browsing of websites have raised demands for high-speed communication. Business services based on HSDPA communication are now being offered, and packet transmission rates as high as 3.6Mbps have been available in Japan since 2006. The top rate was recently raised to 7.2Mbps. HSUPA (High Speed Uplink Packet Access) with the maximum transmission rate of 5.6Mbps is scheduled to be introduced in the near future. As a result, it is expected that more digital contents with high value will be distributed via the cellular phone network. This background has strengthened demands for a truly effective DRM system that can fully protect the contents being delivered.

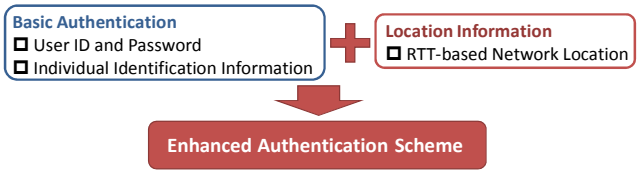

Figure 1. Our authentication scheme

It is necessary to restrict who can access the contents when copyrighted contents are delivered across a public network. There is also a need to control how the contents are used. This topic is involves content management after delivery and is not addressed in this paper. To control access, we need to register users and then authenticate them while they are accessing the content. The authentication technique most generally used involves user ID and passwords. However, given the availability of phishing tools and spyware, malicious users can easily disguise themselves as registered users. It is essential to reinforce the basic authentication step with continuous authentication using information that is unique to the accepted user. We propose to use the location information based on network-based data, presumed here to be the transmission delay between the server and the 3G mobile devices, for authentication. Figure 1 shows the authentication scheme in our DRM system; the 3G mobile device becomes an authentication tool that specifies the individual by registering the place of content access such as the home. Services can be used only in restricted areas such as a university campus and the inside of a museum.

There are two basic approaches to acquiring the user's position: terminal origination and network origination. An example of the former is GPS data. Since this data is held in the terminal there is the possibility of the data being falsified. Since network authentication by means of IP addresses is

978-1-4244-3510-4/09/$25.00 ©2009 IEEE

impossible in 3G mobile devices, we use the transmission delay as measured by the network. The transmission delay changes with network condition but the system can track the changes over time to ensure compliance with the service area limits. [1][2][4][6]

This paper assumes the use of W-CDMA terminals (equivalent to HSDPA) as the 3G mobile devices and clarifies the basic transmission delay characteristics of the corresponding network. An analysis and an experiment show that that the transmission delay is influenced by many parameters. We find that the accuracy with which the transmission delay can be measured depends mainly on the timing of the probing packets. We classify this timing into two modes. We also examine the stability of the minimum transmission delay.

II. Network Configuration and Method of Measuring Transmission Delay

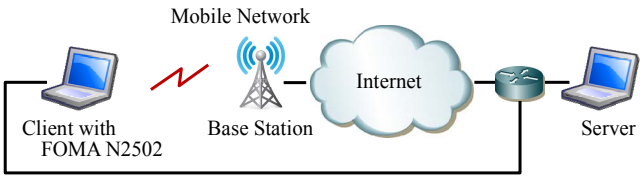

Figure 2. Network configuration

Figure 2 shows the experimental network configuration used to measure the transmission delay. The server is a laptop with Intel Celeron M 1.86 GHz processor and 1GB of memory running Windows Vista. The client is another laptop with Intel Pentium M 1.10GHz processor and 240MB of memory running Windows XP. The client laptop is equipped with a CF type W-CDMA terminal (FOMA N2502 HIGH-SPEED) made by NTT docomo. The W-CDMA terminal offers UL (up link) speed of 384kbps and DL (down link) speed of 7.2Mbps. Here, UL is from the client to the server, and DL is from the server to the client. Between the server and the client, UL throughput can vary from 58 kbps to 362 kbps and DL throughput from 516 kbps to 1.80 Mbps; the number of links was 16. We calculated throughput from our measurement data and used traceroute to measure the number of links.

We measured RTT (Round Trip Time) and OWD (One-Way Delay, UL or DL). In the configuration shown in Figure 2, RTT and OWD can be measured at the same time. We used UDP for the measurement. It is necessary to use three programs on the server side (for sending packets to the client, and for receiving packets from both WAN and LAN) and one program on the client side. When the probe packets are sent or received, we acquire the time stamp information by QPC (Query Performance Counter). Time stamp resolution is determined by QPF (Query Performance Frequency). Because the QPF of the server's PC runs at about 14.3 MHz, system resolution is about 70 ns.

III. Measurement Result

A. Transmission Delay: RTT and OWD

Figure 3 shows typical delay distribution plots of RTT and OWD for the measurement period of 5 minutes. We used port 20 for the RTT measurement and port 2222 for the OWD measurement on the server side; port 20 on the client side was used for both measurements. Unless otherwise specified, subsequent text assumes the use of the same port. The packet size is 116 bytes and the packet sending interval is 100 ms.

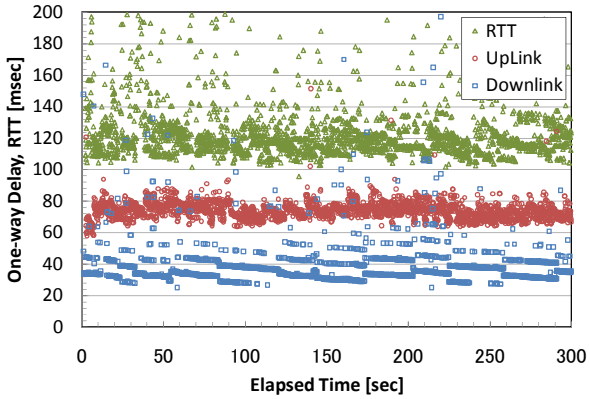

Figure 3. Transmission delay distribution of RTT and OWD

The median value of RTT is about 118 ms. Though RTT in Figure 3 appears to fluctuate randomly, we can find a periodic fluctuation of 20 ms. The median values of UL and DL are about 73.7 ms, and 35.1 ms, respectively. They have different distributions. DL demonstrates a discontinuous delay distribution with 10ms steps while UL exhibits a continuous delay distribution with a 20 ms fluctuation band. The cause of the delay variation is the timing at which the probe packets are loaded into the wireless frame, whose length is 10 ms. The delay is shortest (longest) when the packets arrive just before (after) the wireless frame is transmitted because the packets are sent at once (in the next frame). UL and DL have different kinds of delay distribution because they use different modulation methods. [3]

B. Two Packet Timing Modes

From the data collected in the measurements we clarified that it was critical that the program used to control probe packet release be clearly written so as to specify the timing. To this end, we define the two modes shown in Figure 4.

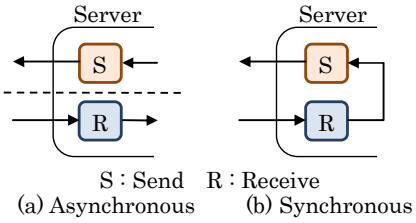

Figure 4. Timing modes for probe packet control

The first is asynchronous mode. The program sending the probe packets and the program receiving the probe packets are run independently and concurrently. The server sends the packets to the client at constant intervals regardless of packet reception. This means that the timing of packet release is not matched to the timing of the wireless system.

The second is synchronous mode. The sending program is linked to the receiving program such that it waits for the reply from the client after sending the probe packet. In this mode, the sending timing becomes set to the timing of the wireless system.

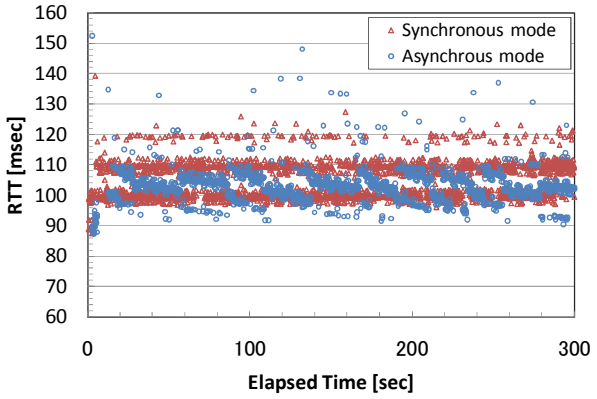

Figure 5. Transmission delay distribution with asynchronous mode and synchronous mode

Figure 5 shows the delay distribution (RTT) in the asynchronous mode and the synchronous mode. The packet size is 44 bytes and the packet sending interval is 100 ms in asynchronous mode. If the packets are sent across the UL and DL by separate timing (asynchronous mode), a continuous delay distribution that is periodic is generated. The fluctuation band in this case is an integral multiple of 10 ms. In synchronous mode, RTT exhibits a non-continuous distribution with 10 ms step size because the frame timing changes in integral multiples of 10 ms due to the delays imposed by the elements forming the network.

C. *Change in Transmission Delay with Parameters*

We changed the parameters of probe packet transmission in asynchronous mode and synchronous mode programs. For the former, the packet size and the sending interval were changed to change the rate. We also measured the result of sending packets in burst. For the latter, we inserted some delay before the next probe packet was transmitted from the server. We also examined burst-transmission. When we changed the packet size in synchronous mode, the change was confirmed to match that seen in asynchronous mode. [5]

Figure 6 shows the transmission delay versus packet size. We used asynchronous mode, and the packet sending interval was 100 ms. The transmission delay increases with the packet size. The cause of this change is the packet processing time.

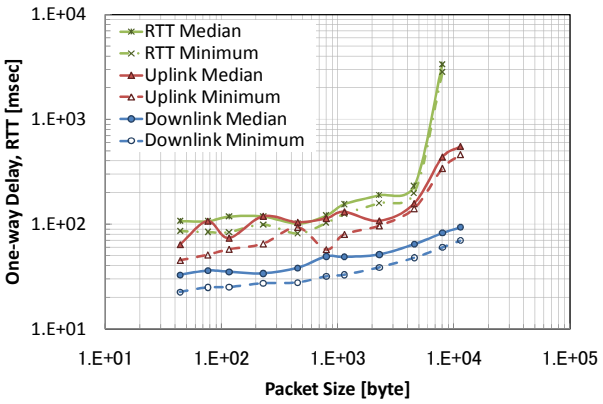

Figure 6. Transmission delay versus packet size

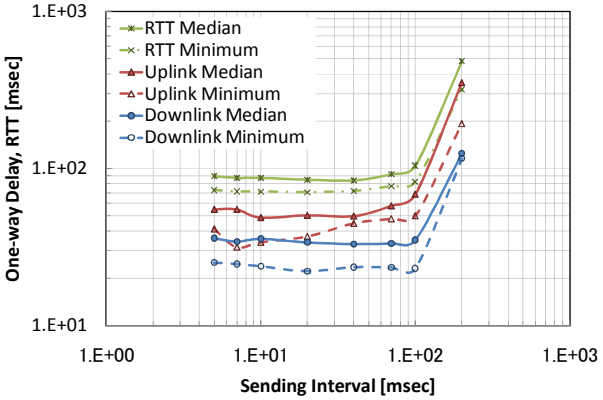

Figure 7. Transmission delay versus sending interval

Figure 7 shows transmission delay versus the sending interval. We used asynchronous mode, and the packet size was 44 bytes. When the sending interval is 100 ms or less, the transmission delay is basically constant. At larger intervals, however, the delay increases rapidly. A similar phenomenon was confirmed at several measurement sites. The cause for this delay increase is the packet processing time.

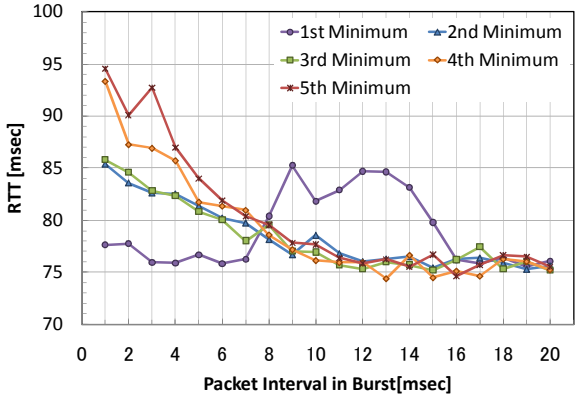

Figure 8. Transmission delay versus packet sending interval in the burst (asynchronous mode)

Figure 8 shows the transmission delay versus the packet sending interval in burst style transmission. We used asynchronous mode, and the packet size was 44 bytes; there were 5 packets per burst, and the burst interval was 100 ms. In Figure 8, we pay attention to only the minimum value of RTT of each packet. In burst-transmission (100 ms interval), the packets have almost the same minimum RTT for sending intervals from 16 ms to 20 ms. This is because the sending timing is adjusted by the sending interval in the burst.

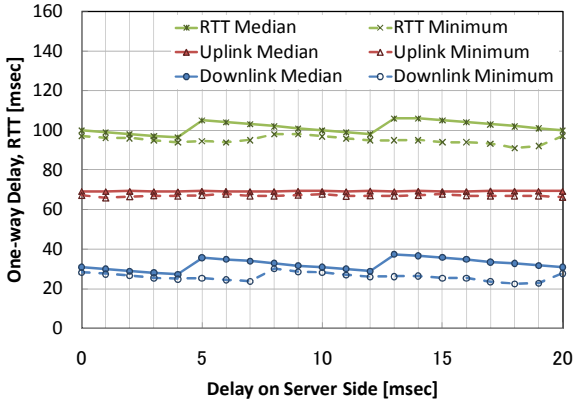

Figure 9. Transmission delay versus inserted delay value

Figure 9 shows the transmission delay versus the delay inserted when the packets are transmitted on the server side. We used synchronous mode, and the packet size was 44 bytes. UL delay is constant regardless of the delay inserted, unlike DL and indeed RTT. The reason for this is that the sending interval is altered by the value of the delay inserted. The transmission delay is minimized when the timing of probe packet insertion is optimized.

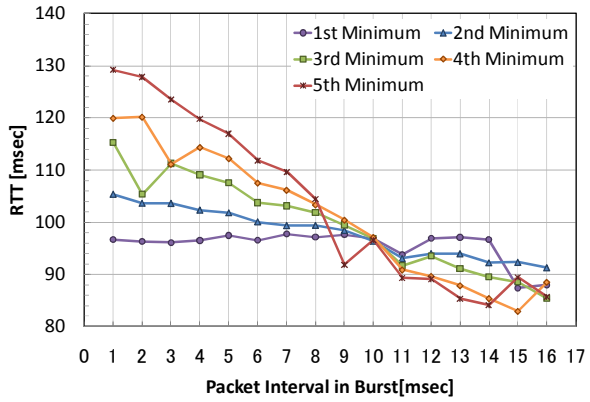

Figure 10. Transmission delay versus packet sending interval (synchronous mode, burst transmission)

Figure 10 plots the transmission delay versus the packet sending interval (burst transmission). We used the synchronous mode, and the packet size was 44 bytes; there were 5 packets per burst. In Figure 10, we pay attention to only the minimum value of RTT of each packet. When the sending interval in the burst was less than 10 ms, the RTT of the 1st packet was the smallest, and the following packets (from 2nd to 5th) yielded a steady increase in RTT. When the sending interval was 10 ms, the RTT of each packet basically became equal. When the sending interval was larger than 10ms, the minimum RTT of the following packets gradually became small. At the median RTT, a similar change was confirmed across the boundary of 10 ms, and the median RTT of the 1st packet was basically constant. These characteristics occur because the sending interval is adjusted as occurs in the asynchronous mode case.

As shown above, many parameters, such as packet size, sending interval, burst/non-burst transmission, delay insertion and so on, influence the transmission delay.

D. Stability of Minimum RTT

In implementing the RTT-based authentication scheme, there is a trade-off between the stability and the measurement time. Figure 11 shows the stability of minimum RTT versus observation time. We extracted the minimum value every second. Synchronous mode yielded the best stability. For example, the stability was about 200 us in the first 10 seconds. We should find a method that alters the parameters so as to raise the stability of minimum RTT.

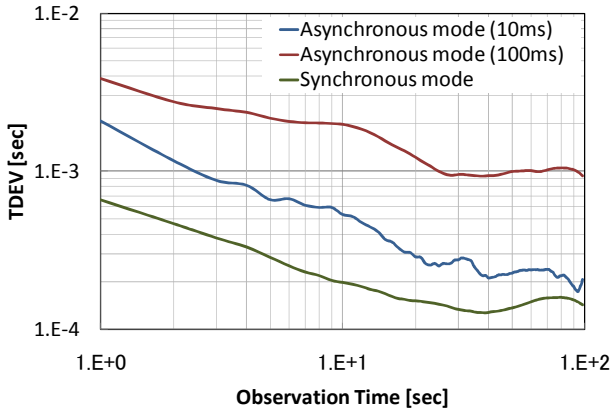

Figure 11. Stability of minimum RTT versus observation time

IV. SUMMARY AND CONCLUSION

We executed some measurements to use the transmission delay for location information. We clarified the basic transmission delay characteristics of the corresponding network with W-CDMA terminals (equivalent to HSDPA). We found that there were two modes for probe packet control from the data collected in the measurements. These two modes are synchronous mode and asynchronous mode. Their transmission delay characteristics are completely different. We investigated the influence of many parameters, such as packet size, sending interval, burst/non-burst transmission, delay insertion and so on, on the transmission delay in the two modes. We also examined the stability of the minimum RTT. The minimum RTT was steady in the synchronous mode and its stability was about 200 us.

REFERENCES

[1] F. Hartung and F. Ramme, "Digitals Rights Management and Watermarking of Multimedia Content for M-Commerce Applications," IEEE Communications Magazine, Nov.2000, pp. 78-84.

[2] M. Kihara, N. Ohta, and S. Ono, "A New DRM Scheme Based on Uniquely-Identified Content with Ubiquitous Authentication," Proceedings of WPMC '06, September 2006, USA.

[3] J. Prokkola, M. Hanski, M. Jurvansuu, M. Immonen, "Measuring WCDMA and HSDPA Delay Characteristics with QoSMet," IEEE Communications Society, ICC 2007.

[4] J. Berena, M. Kihara, N. Ohta and S. Ono, "A New DRM Scheme Based on Location Enforcement," Proceedings of the ENC-GNSS '07, May 2007, Geneva.R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[5] J. Berena and M. Kihara, "An Experimental Analysis of Packet Train Probe for a Stable RTT Measurement," IEICE Electronics Express, Vol.4, No. 24, December 2007.

[6] J. Berena, M. Kihara, N. Ohta and S. Ono, "Location-based Authentication Scheme for a DRM System Using a Mobile Device," Proceedings of the ENC-GNSS 2008, GPB00 - 032, May 2008, Toulouse.