Impact Transport Layer Protocol Performances to the Encrypted Traffics

S Suherman, Sihar P Panjaitan, Andi Gunanta Ginting

Universitas Sumatera Utara, Medan 20155, Indonesia
suherman@usu.ac.id

Abstract. Transport layer protocols either reliable or unreliable are prone to packet losses. Data transmitted by these protocols are either encrypted or not. The encrypted or compressed traffics are sensitive to losses. Often packet losses lead to failure in extracting the encrypted messages. This paper evaluates the impact of those packet losses on transport layer protocols to the encrypted traffics. The NS-2 simulator is employed and some encryption algorithms are examined. As results, the percentage of successful decryption on TCP is higher than UDP. The higher the packet loss rates the lower the decryption rates. 3DES is more immune to packet losses than Rijndael and Arcfour. In average, it decrypted the encrypted messages 0.38% higher than Rijndael and 0.12% higher than Arcfour.

1. Introduction
Transmission Control Protocol (TCP) guarantees data transmission by using acknowledgement services [1]. This leads to retransmission to the lost packets. On the contrary, User Datagram Protocol (UDP) sends data without confirmation which leads to higher packet loss than TCP. Acknowledgement and retransmission schemas on TCP produce additional delay which unsuitable for delay sensitive applications. On the other hand, UDP data streaming losses packets that is unsuitable for packet loss sensitive applications [2].

Both TCP and UDP protocols are often combined producing new protocols. Some protocols are design to take advantages of UDP but applying some TCP properties to the designed protocols [3, 4]. Other protocols apply error correction to avoid retransmission [5, 6]. Some streaming protocols implement TCP for data control messages, and use UDP for data streaming [7].

In terms of application data, the encrypted and compressed information are sensitive to loss packets. Packet loss on these data often leads to failure decryption. Some important applications such as email, e-commerce and file transfer protocol rely on TCP for their end to end transmission. Even dough, the transport layer protocols are prone to experience loss packets. Even dough TCP counts on retransmission schema, the multiple network errors are still producing losses. Therefore, this paper examines how far the loss packets on transport layer protocol impact the encrypted message transmission. The paper is organized as follows. The assessment for the encrypted data transmission is outline in research method. Some encryption algorithms are applied. Results of transmission using UDP and TCP are reported in section results and analysis, followed by the conclusion.

2. Methodology
In order to examine transport layer losses impact on the encrypted message transmission, the network simulator (NS-2) [8] is employed. In order to trace the network performance parameters, Evalvid framework [9] is inserted to NS-2 code. As the primary intention is to examine packet loss impact, the 802.11 infrastructure is chosen as wireless network is more interference and noise sensitive than wired network. Further, the ad hoc infrastructure is selected.
The assessed 802.11 network consists of mobile nodes from 2 to 20 as depicted in Figure 1. Traffics were sent one way to the one of the node so that collision probability increases and simulation is under the worst packet loss probability. Traffic is generated from a text file, encrypted by using Arcfour, Rijndael-192 and 3DES [10].

The cypher texts are then chopped into packets with size of 160 bits. Each cypher text slice is loaded to a 1024 byte length of TCP segments or UDP datagrams. In the end of simulations, the lost packets generated by Evalvid traces are used to skip the corresponding cypher text slices. Afterwards, the generated received messages were decrypted by using the corresponding decryption algorithm.

3. Results and discussion

The average values are delay, jitter and packet loss characteristics of the encrypted messages transmitted through 802.11 networks by using number of nodes from 2 to 20 nodes for each encryption method have similar pattern. These parameters are represented by arcfour data.

TCP produces higher delay than UDP. Delay is caused mainly by acknowledgment of the transmitted packet. This paper uses window size 1 which means the next packet transmission is processed when the previous packet acknowledgement arrives. Both delay lines increase linearly. TCP gradient is twice of UDP gradient. For both protocols, delay increases slowly from 2 ms to about 20ms for node number less than 6. But then it increases significantly as node number increases. TCP average delay is 82.4 ms. UDP is 41.7 ms. Delay pattern is depicted in Figure 2.

The jitter pattern for TCP and UDP is shown in Figure 3. Jitter increases as number of node arises. Since TCP sends packet smoothly after waiting for the acknowledgement packet, its jitter changes regularly from 0.5 ms for number of nodes 2 to 28.4 m for number of nodes 20. On the other hand, UDP floods network with packets which results network congestion. Its average jitter is higher than TCP. The average TCP jitter is 16 ms while UDP is 21.7 ms.
As explained previously, TCP sends packets very smoothly as each packet is sent only if the previous packet acknowledgement is received. This tidy packet scheduling results the high probability of successfully transmitted data. On the contrary, UDP floods network with packets. UDP transmitter within transport layer does not care to the capability of medium access layer. As result, the sending node may fail sending UDP packets.

As depicted in Figure 4, the capability of node in sending data is much lower than TCP. The failure rates increase as number of nodes in the same network increases. The successful data transmission on TCP decreases from 100% at 6 nodes to 97% at 20 nodes. In contrast, UDP achieves only 99% for 2 nodes down to 92% at 18 nodes. TCP successfully send 99.27% of data, UDP sends 96.44% data (Figure 4).

The next parameter is packet loss (Figure 5). UDP experiences higher packet loss than TCP. Its packet loss increases from 1% at 2 nodes to 5.7% at 20 nodes. This low packet loss rates in a crowded network with up to 20 nodes because the rates of the transmitted data is low, about 1024 bytes every 4 ms or 200 kbps. Even dough, the figure shows that in average, UDP has 3.6% losses while TCP is only 0.7% losses.

The successfully received packets are then reconstructed and decrypted by using the related algorithm. The Arcfour algorithm I successfully decrypting messages up to 99.32% for TCP and 64.4% for UDP. As shown in Figure 6, TCP is able to decrypt almost 100% up to number of node 18, then down to 97% at 20 nodes. UDP hold almost 100% only up to 6 nodes, it fluctuates when nodes higher than 6.
Rijndael-192 (Figure 7) and 3DES (Figure 8) experience the same pattern as Arcfour, where TCP causes decryption rate higher than UDP. TCP with Rijndael-192 algorithm is successfully decrypting 99.19% data while UDP is only 64%. The 3DES algorithm generates 99.44% of the original messages for TCP and 64.5% for UDP. Figure 9 shows the successful decryption rates for all algorithm using both TCP and UDP. TCP produces successful 99.31% original messages in average. It is 35.03% higher than UDP which is about 64.28%. Among the three algorithms, 3DES is the most powerful algorithm dealt with packet losses. 3DES successfully decrypts the encrypted messages 0.38% higher than Rijndael and 0.12% higher than Arcfour.

4. Conclusion
To conclude, the TCP delay is higher than UDP, TCP results 82.4 ms delay almost twice of UDP delay. However TCP jitter is lower than UDP as TCP sends data smoothly (TCP jitter is 16 ms while UDP is 21.7 ms). UDP experience higher loss about 3.6% but TCP loss is only 0.7%.

TCP and UDP losses are proportional to decryption rates. The Arcfour algorithm successfully decrypts messages up to 99.32% for TCP and 64.38% for UDP. Rijndael-192 algorithm decrypts 99.19% data for TCP and 63.97% for UDP. TCP produces successful 9943% original messages by using 3DES and only 64.49% for UDP. It is clearly shown that higher losses on UDP causes lower decryption rate. Comparing the three encryption methods, 3DES is the most powerful algorithm dealt with packet losses. 3DES successfully decrypts the encrypted messages 0.38% higher than Rijndael and 0.12% higher than Arcfour. Further work may propose the technique to increase decryption rate further.

References
[1] M. Al-Akaidi, “A review on transport layer protocol performance for delivering video on an adhoc network,” in IOP Conference Series: Materials Science and Engineering, 2017, p. Vol. 237, No. 1, 012018.
[2] S. Marwan Al-Akaidi, “A transport layer protocol for uplink WiMAX video streaming,” Int. J. Multimed. Ubiquititous Eng., vol. 10, no. 1, pp. 19–32, 2015.
[3] K. Huh, J. H., & Seo, “RUDP design and implementation using OPNET simulation..” in Computer science and its applications, 2015, pp. 913–919.

[4] M. Suherman, S., & Al-Akaidi, “Increasing uplink broadband video streaming protocol performance in WiMAX network.” Int. J. Internet Protoc. Technol., vol. 7, no. 3, pp. 176–185, 2013.

[5] T. Fairhurst, G., & Jones, “Transport Features of the User Datagram Protocol (UDP) and Lightweight UDP (UDP-Lite).” 2018.

[6] N. Abdurrahman, H., Sitompul, O. S., & Mubarakah, “UDP-Lite Enhancement Through Checksum Protection.” IOP Conf. Ser. Mater. Sci. Eng., vol. 180, no. 1, p. 12146, 2017.

[7] M. A. Hajer, “Examining RTP Traffic in Multimedia Conferencing System over TCP and UDP,” J. Wirel. Netw. Commun., vol. 7, no. 2, p. 31–34., 2017.

[8] E. Issariyakul, T., & Hossain, Introduction to network simulator NS2. Springer Science & Business Media., 2011.

[9] J. Klaue, B. Rathke, and A. Wolisz, “Evalvid—A Framework for Video Transmission and Quality Evaluation,” in 13th International Conference, TOOLS 2003, Urbana, IL, USA, September 2-5, 2003. Proceedings, 2003, no. September, pp. 255–272.

[10] D. Furht, B., & Kirovski, Multimedia security handbook. CRC press., 2004.