Impact encryption algorithm used in three pass protocol for securing WiMAX link

Suherman

Electrical Engineering Department, Universitas Sumatera Utara, Medan-Indonesia

*suherman@usu.ac.id

Abstract. Wireless network is popular for internet connection. WiMAX provides higher bitrates connection compared to the popular 802.11 network. Since wireless link is more security risk than the wired one, solutions for securing the wireless link are often proposed by many researchers. Since WiMAX link employs contention request for best effort service which lead to higher delay, security solution should not inject excessive link delay. This paper examines the use of three pass protocol (TPP) in transferring the encryption keys. One time pad protocol (OTP) is the basic key encryption within TPP. Since OTP is a simple XOR key, its protection is weak. This paper compares link delay produced by more advance encryption techniques when replacing OTP within TPP. Simulation shows that with the security increment, blowfish encryption produced the lowest link delay increment lower than 150 ms. While AES, 3DES and DES results excessive delay.

1. Introduction

Worldwide interoperability microwave access (WiMAX) provides high bit rate wireless link for internet connection. Its speed and coverage are even higher than wifi network. WiMAX compliances to IEEE 802.16 standard with variants for fixed point to point mode [1], mobile mode [2], and 4G compatible network [3]. WiMAX provides quality of services (QoSs) negotiation and enforcement [4] with advanced security features [5].

Users often apply the security protocol to their application even dough network has provided it, since some issues related to network security have been reported [6]. One of ways in securing data over wireless link is by using encryption algorithm. This algorithm requires key sharing techniques that are mostly developed based on the three pass protocol (TPP) key sharing [7]. TPP transfers encryption key by using the three messages as shown in Figure 1. The description assumes key is exchanged from Anton to Beby [a]. Password is treated as a text and encrypted by key A in Anton. The cipher text is transmitted to Beby. Beby encrypts this message using key B and sends it back to Anton. Upon reception, Anton decrypt the message leaving encrypted key by using key B. This message is finally sent to Beby and decrypted by Beby to get the key. Some works replace the OTP by using other encryption algorithm such as H-Rabin [8], Hill [9], Viginere [10] and El-Gamal [7] or even applied modification partially [11].

For high QoS users, link delay may not be an issue, but for best effort users who request services using contending method, delay is sometimes matter [12]. Therefore, additional security solution from users should not add excessive delay, moreover if the link service is best effort. Some works have examined the encryption performance comparisons [13] and impact losses to encrypted data [14]. This paper examines OTP improvement impact to the wireless link delay, mainly for WiMAX with best effort users.
2. Research Method
In order to examine WiMAX link delay due to TPP implementation with various OTP replacements, the NS-2 simulations were performed by using NIST WiMAX module. Although the provided simulator has maximum throughput of 7 Mbps, the limited number of subscriber stations (SSs) is used as plotted in Figure 2. With wireless coverage radius is set about 1000 m, the 64 QAM modulation is expected to efficiently deliver traffic traces of 500 kbps sent by four SSs. The main examined parameter is the transmission time from SSs to a receiving station connected to base station (BS). Delay is calculated from each packet sent by SS using the transmission control protocol (TCP). The transmission delay is set when TCP packet is sent, and the receiving time is recorded when TCP packet is received. The examined key encryption algorithms are OTP, DES, 3DES, AES and Blowfish.

3. Simulation results
Separate assessment shows that blowfish (BF) requires the smallest encryption time as depicted by Figure 3 with average time is 0.628 ms per byte for input length of 10 to 100 bytes. AES has the longest time with average encryption time of 1.256 ms. This has also been demonstrated by other researchers [13] for assessment of higher block sizes. The decryption assessment shows decryption delay is higher than encryption.

![Figure 3. Transmission delay of encrypted information with TPP.](image)

As the encryption method applied to replace the OTP within TPP, the link delay increases in various degree as plotted in Figure 4. In average, the link delay increment reaches 118.81% for AES encryption algorithm, followed by 125.80%, 138.79% and 77.23% for DES, DES and BF subsequently. BF exerts the lowest delay increment giving 133.226 ms in average. The delay increments of AES, 3DES and DES are higher than the standard delay for real-time traffic (150 ms) [15]; meanwhile BF poses the expected level.

![Figure 4. Transmission delay of encrypted information with TPP.](image)

4. Conclusions
This paper has examines link delay when various encryption techniques applied in WiMAX link with contending users. The OTP exerts the lowest delay (75.17 ms), but this technique has weakness as key is failed if the three TPP messages are captured by the third party. The BF encryption produces the lowest delay, 133.226 ms in average, while AES, 3DES, and 3DES have higher delay than the standard. To conclude, it is not recommended to use excessive delay encryption algorithm in three pass protocol, as it will increase wireless link delay in passing encryption key. Excessive delay makes average delay is higher than the recommended delay for real-time application. Moreover if key is changed dynamically.

References
[1] IEEE Std. 802.16-2004, Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE, October 2004.

[2] IEEE Std. 802.16e-2005, Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Dec. 2005.

[3] IEEE Std 802.16m-2011, Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems, IEEE, pp.1-1112, May 5, 2011.

[4] Vu H L, Chan S, Andrew L. 2010. Performance Analysis of Best-Effort Service in Saturated IEEE 802.16 Networks. IEEE Trans. on Vehicular Technology, 59(1), 460-472.

[5] Ahson S A, Ilyas M. 2018. WiMAX: Standards and security. CRC press.

[6] Kumar C, Arya Y, Agarwal G. 2018. A review Report on WiMAX Vulnerabilities, Security Threats and their Solutions. Second International Conference on Inventive Communication and Computational Technologies (ICICCT) 1963-1967.

[7] P. S. Agung, S. Efendi, S. Suherman, “Improving One-Time Pad Algorithm on Shamir’s Three-Pass Protocol Scheme by Using RSA and ElGamal Algorithms”, International Conference on Computing and Applied Informatics, 2018.

[8] D. Rachmawati, M. Andri Budiman, “An Implementation of the H-Rabin Algorithm in the Shamir Three-Pass Protocol”, 2nd International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT), 2017.

[9] A. P. Utama Siahaan, “Three-Pass Protocol Concept in Hill Cipher Encryption”, Seminar Nasional Aplikasi Teknologi Informasi (SNATi), ISSN: 1907 5022, 2016.

[10] A. Subandi, R. Meiyanti, C. L. Mestika Sandy, R.W. Sembiring, “Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification”, Advances in Science, Technology and Engineering Systems Journal, Vol. 2, No.5, 1-5 2017.

[11] A Badawi, M Zarlis, S Suherman, “Impact three pass protocol modifications to key transmission performance”, International Conference on Computing and Applied Informatics, 2018.

[12] Suherman, S. (2018). Delay reduction of transmission control protocol in WiMAX by prioritizing the acknowledgement packets. In MATEC Web of Conferences (Vol. 197, p. 11021). EDP Sciences.

[13] Al Tamimi, A. K. (2013). Swati.,” Performance Analysis of Data Encryption Algorithms “, International Journal of Advanced Research in Computer Science and Software Engineering, 3(2), 147-149.

[14] Suherman, S., Panjaitan, S. P., & Ginting, A. G. (2019, June). Impact Transport Layer Protocol Performances to the Encrypted Traffic. In Journal of Physics: Conference Series (Vol. 1235, No. 1, p. 012032). IOP Publishing.

[15] ETSI, D. (1998). TIPHON-05001, Telecommunications and Internet protocol harmonization over networks (TIPHON); General Aspects of quality of service (QoS). TR 101 329 Ver. 1.2. 5, October.