Journal of Engineering and Applied Sciences 13 (Special Issue 2): 2946-2950, 2018
ISSN: 1816-949X

Timestamp-based Key Exchange Protocol in Satellite Environment

[1]In-A Song, [1]Young-Seok Lee and [2]Hoon Choi
[1]Department of Information and Telecommunication Engineering, Kunsan National University, 54150 Kunsan, Koera
[2]Department of Computer Engineering, Chungnam National University, 34134 Daejeon, Koera

Abstract: The satellite communication is easily exposed to attacks like eavesdropping of information, abnormal sending of packet, reusing of message, forgery/alteration of data, etc. To prevent these attacks, key exchange protocol is conducted between NCC (Network Control Centre) and RCST (Return Channel Satellite Terminal). ETSI (European Telecommunication Standards Institute) designed main key exchange protocol exchanging keys through cookie-based user authentication. Exposure of data at the early time when NCC and RCST exchange cookies, however, brings man-in-the-middle attack. Replay attack is also possible because it doesn't make any encryption during data transmission. Though certificate-based protocol was suggested to prevent Man-in-the-middle attack, it is not appropriate for satellite environment. This study suggest the protocol which can prevent man-in-the-middle attack using time stamp and compare the proposed protocol with existing protocols through performance analysis/evaluation, showing its resource management and the efficiency of communication.

Key words: Diffie-Hellman, key exchange protocol, time stamp, satellite communication, NCC, ETSI

INTRODUCTION

The current satellite communication is easily exposed to attacks like eavesdropping of information, abnormal sending of packet, reusing of message, forgery/alteration of data, etc. To prevent these attacks, the satellite communication has inside/outside network security policies and these policies should be able to offer security services including authentication, confidentiality of data, availability, integrity and unmanned prevention.

A way used to satisfy above matters is encryption/decryption and authentication of data using the key. For safe key exchange there exist key exchange protocol presented from EN 301 790 the standard of ETSI (European Telecommunication Standards Institute) and Certificate-based protocol made by improving previous protocols (Lee, 2013; Chang and Chang, 2005).

Figure 1 shows the satellite reference model for broadband network. NCC (Network Control Centre) means the center of network maintenance and RCST (Return Channel Satellite Terminal) means the satellite terminal of the user. Key exchange protocol is conducted between NCC and RCST (ETSI., 2009).

As existing key exchange protocols have risks to be exposed to attacks, however, it is hard to see that they are safe. The basic key exchange protocol of EN 301 790 standardized in the international standard institution ETSI is Main Key Exchange (MKE). It conducts exchanging keys through cookie-based user authentication. Exposure of data at the early time when NCC and RCST exchange cookies, however, brings man-in-the-middle attack.

This study suggests key exchange protocol for preventing man-in-the-middle attack by introducing timestamp to improve the disadvantages of existing protocols. Like MKE protocol because it uses Diffie-Hellman key exchange method it requires the calculation process of the public key in NCC and RCST. NCC creates timestamp during transmitting/receiving data and identifies man-in-the-middle attack by using calculation time of the public key of NCC and RCST. Plus, its usage of time stamp whose data size is small makes itself free from the problem of resources against existing protocols.

Literature review: "There are several types of existing key exchange protocols based on satellite network, MKE protocol of ETSI standard EN 301 790, quick key exchange protocol conducting only authentication without exchanging data for quick key exchange, explicit key exchange protocol exchanging the common key with several RCSTs, certificate-based key exchange protocol

Corresponding Author: Young-Seok Lee, Department of Information and Telecommunication Engineering, Kunsan National University, 54150 Kunsan, Koera

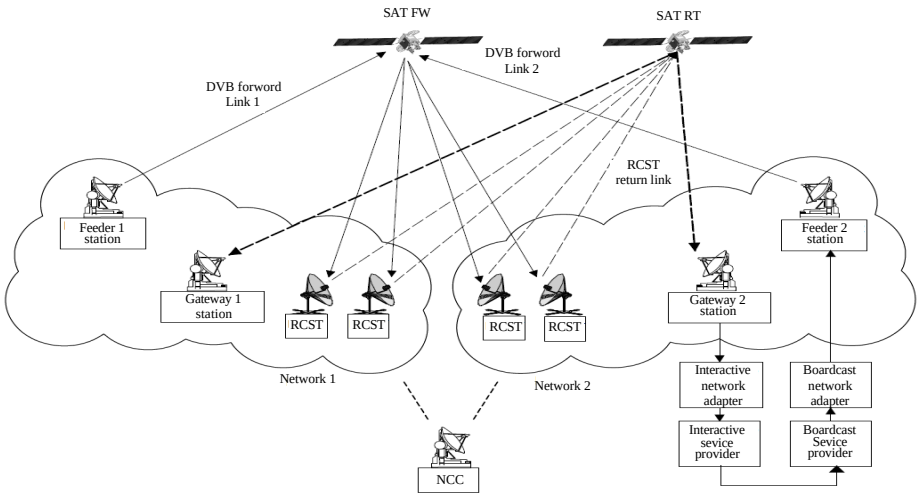

Fig. 1: Reference model for the satellite interactive network

improving MKE protocol, improved protocol using MTI key exchange protocol and improved protocol using elliptic curve method.

MKE is the basic key exchange protocol of EN 301 790 standard (ETSI., 2009). It uses diffie-hellman algorithm for sharing the secret value between NCC and RCST and uses the cookie value, so that, RCST can make the user authentication to NCC. It is the protocol conducted every time a new session is set and uses selectively the shared value made newly for renewal of the cookie value. Finally, it derives the shared secret key to create ciphertext for processing payload stream data. In MKE protocol, there can be man-in-the-middle attack and replay attack. At the early time, the cookie value is setting if an attacker transmits and authenticates the public value between NCC and RCST using the obtained cookie value after gaining the cookie value from an adversary, the attacker can share both secret values of NCC and RCST.

Therefore , NCC and RCST exchanging cookies at the first implementation of session are exposed to man-in-the-middle attack. Plus, though it exchanges cookies safely, the number of cookie NCC must manage increases according to the number of RCST, leading to rapid increase of memory usage. So, it can't be seen the efficient protocol overall.

When it comes to replay attack because RCST transmits without encrypting such data as the random number of NCC (NONCE 1), the random number of RCST (NONCE 2) and the authentication value using hash function (auth(r)) for authentication, the attacker can disguise as RCST through retransmitting the obtained data in session after gaining data.

In order to overcome disadvantages of MKE protocol examined above, certificate-based protocol was suggested (Roy-Chowdhury and Baras, 2008; Fang and Jiulun, 2013). Because, it uses the public value for a long time using certificates, it introduces the random number for the freshness of secret. Unlike MKE protocol, for reliability of the secret key changed by every session, it uses the second authentication value. The second authentication value calculates the secret value every session by performing existing Diffie-Hellman algorithm using the arbitrary random number value and the public value of adversary. So, if the arbitrary random number value changes, the private value also changes and the freshness of secret can be offered. Also, key reliability can be guaranteed because the authentication procedure is offered in the protocol.

Certificate-based protocol, however, requires additionally the process NCC and RCST should identify mutual certificates for authentication, thereby increasing the communication amount of satellite communication and the computation amount of the device. This can't be seen an effective method in wireless communication which has lots of restriction unlike cable communication.

MATERIALS AND METHODS

The suggested protocol: MKE protocol of EN 301 790 standard of ETSI is vulnerable to man-in-the-middle attack and replay attack and the certificate-based protocol isn't efficient in the satellite communication because it uses the certificate. In order to complement these disadvantages, this study suggests the protocol which can identify the

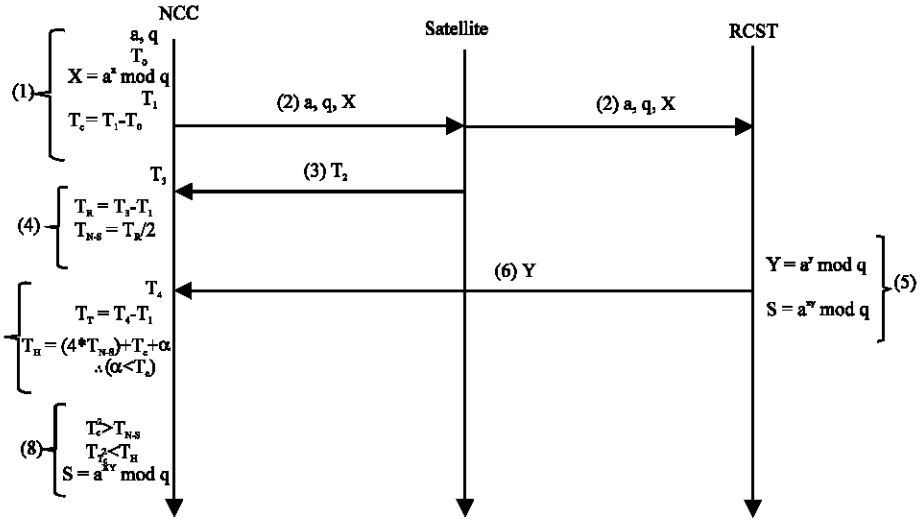

Fig. 2: Proposed protocol

Table 1: Protocol parameters

Notations	Descriptions
a, q	Prime numbers for Diffie-Hellman operation
x	Private value of NCC
y	Private value of RCST
X	Public value of NCC
Y	Public value of RCST
S	Secret key created by NCC and RCST
T_C	Computation time to create public value X of NCC
T_R	Round-trip time between NCC and satellite
T_{N-S}	Transmission time from NCC to satellite
T_T	Round-trip time between NCC and RCST
T_H	Round-trip threshold time between NCC and RCST
T_0	Time value before public value computation of NCC
T_1	Time value after public value computation of NCC
T_2	Time value when satellite receives values of NCC
T_3	Time value when NCC receives time-stamp of satellite
T_4	Time value when NCC receives public value Y of RCST

attack without data shared by NCC and RCST and have less amount of communication and computation of the device than when the certificate is used.

It uses Diffie-Hellman algorithm for generating the secret key and applies timestamp for preventing man-in-the-middle attack. Never using the fixed public value, the suggested protocol can have freshness of the key and guarantee the reliability of the key thanks to offering its authentication procedure. Table 1 shows the system parameter used in the suggested protocol. Figure 2 represents flowchart of the suggested protocol which is performed in the total eight-step procedure.

After deciding Diffie-Hellman prime numbers a, q, NCC generates timestamp T_0. After calculating the public value X with the private value x and prime numbers a, q, NCC transmits prime numbers a, q and the public value X to satellite, generating timestamp T_1. For arithmetic operation time of the public value T_C, T_1-T_0 = T_C is calculated. The satellite receives a, q, X and transmits them to RCST. After calculating timestamp T_2 receiving a, q, X, the satellite transmits it to NCC. NCC receives timestamp T_2 and generates timestamp T_3 to confirm time receiving T_2. In order to confirm the round-trip time between NCC and the satellite (T_R), T_3-T_1 = T_R is calculated and then $T_R/2 = T_{N-S}$ is gained. RCST receiving a, q, X generates the public value Y using its own private value y and prime numbers a, q. After sending the public value Y to the satellite, RCST calculates the secret key S using the received public value X of NCC and its own public value Y. The satellite receiving the public value Y from RCST transmits it to NCC. NCC receiving the public value Y generates timestamp T_4 to confirm reception time and then T_4-T_1 = T_T is calculated for round-trip time between NCC and RCST. To obtain round trip threshold time between NCC and RCST, $(4*T_{N-S})+T_C+\alpha = T_H$ is calculated. Here, α as variable time should not be set larger than calculating time of the public value (T_C). In order to confirm man-in-the-middle attack, NCC judges its existence by using timestamp. First to confirm man-in-the-middle attack between NCC and satellite, it should be checked whether calculating time of the public value T_C is larger than transmission time between NCC and satellite T_{N-S} ($T_C > T_{N-S}$). In case that transmission time T_{N-S} is larger than calculating time of the public value T_C, it is judged that man-in-the-middle attack is conducted, so, the protocol process ceases. In case that the first step is true

to confirm man-in-the-middle attack between satellite and RCST, it should be checked whether round-trip time between NCC and RCST T_T is smaller than round-trip threshold time T_H(T_T<T_H). In case that T_T is larger than T_H, it is judged that man-in-the-middle attack is conducted, so, the protocol process ceases. If both the first and second judging processes are true, NCC calculates the secret key S using its own public value X and the public value Y of RCST.

RESULTS AND DISCUSSION

Performance evaluations: To analyze the efficiency of the suggested protocol and the previous protocols, a simulation was conducted using NS-2. The environmental option was used as the most usable one during setting of NS-2 satellite simulation and the satellite channel was set according to basically supplied channel/sat.

Each key exchange protocol consists of totally four-step network transmission. Because two terminals pass through the geostationary satellite in the middle of sending data, the process is the same as following from source (src) terminal to the satellite from the satellite to destination (dst) terminal from dst terminal to the satellite and from the satellite to src terminal. Table 2 shows the size of the parameter used in this simulation. The size of parameter was determined with ETSI method and generally-used method.

When it comes to communication in case of conducting protocols up to 1000 sec, MKE protocol is about 172 KB because of the prime numbers for diffie-hellman process and the public value of NCC and RCST. Certificate-based protocol shows the biggest amount as about 196 KB because it uses the certificate during transmission of the public value. In case of the suggested protocol, however, it consists of timestamp whose packet size is small, so, its communication amount is shown to be the smallest as about 113 KB in Fig. 3.

As for computation, MKE protocol and certificate based protocol shows the similar amount at first but with the passage of time, it can be confirmed that computation of certificate-based protocol is larger than that of MKE protocol as shown in Fig. 4. In case of the suggested protocol, unlike other protocols, it shows the smallest computation because there is no additional calculation for hash computation or the certificate.

Table 2: Simulation parameters

Values	Algorithm	Key size (bit)	Output size (bit)	Method
Key exchange	Diffie-Hellman	512	512	ETSI
Hash	HMAC-SHA1	-	160	ETSI
Random number	Pseudo	-	64	ETSI
Timestamp	-	-	32	General

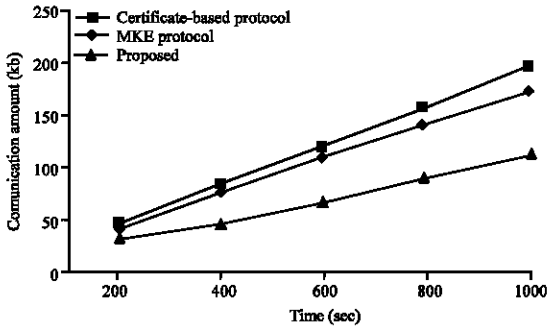

Fig. 3: Comparison of communication amount

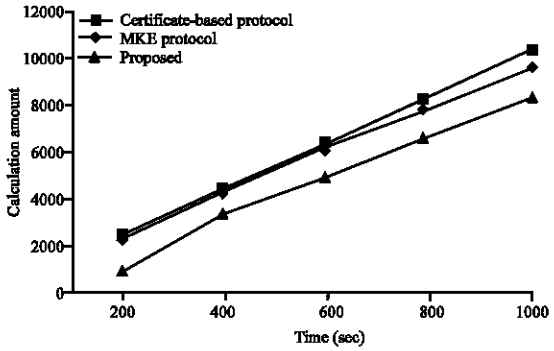

Fig. 4: Comparison of computation amount

CONCLUSION

This study suggested the protocol which can prevent man-in-the-middle attack using timestamp and compared this with existing protocols through capacity analysis/evaluation, showing its resource management and the efficiency of communication resources. The procedure of preventing man-in-the-middle attack of the suggested protocol was examined through safety analysis and it was represented that it can prevent replay attack with addition of ID parameter. If the suggested protocol is applied in accordance with the operational environment, it can be expected to be a very efficient protocol in the satellite communication using existing NCC and RCST.

ACKNOWLEDGEMENTS

This research was supported by ICT Promising Technology Development Program of Institute for

Information and Communications Technology Promotion (IITP) funded by the Ministry of Science, ICT and Future Planning (Grant R6910-15-1102). Hoon Choi was supported by the IT R and D program of MOTIE/KEIT. [10049270, SoC-SW platform for computer-vision based UI/UX on wearable smart devices].

REFERENCES

Chang, Y.F. and C.C. Chang, 2005. An efficient authentication protocol for mobile satellite communication systems. ACM. SIGOPS Operating Syst. Rev., 39: 70-84.

ETSI., 2009. Digital Video Broadcasting (DVB): Interaction channel for satellite distribution systems: Guidelines for the use of EN 301 790. Technical Report ETSI TR 101 790 V1.4.1 (2009-07). http://www.etsi. org/deliver/ etsi_tr/101700_101799/101790/01.04.01_60/tr_101790 v010401p.pdf.

Fang, R. and F. Jiulun, 2013. An adaptive distributed certificate management scheme for space information network. IET. Inf. Secur., 7: 318-326.

Lee, C.C., 2013. A simple key agreement scheme based on chaotic maps for VSAT satellite communications. Intl. J. Satell. Commun. Netw., 31: 177-186.

Roy-Chowdhury, A. and J.S. Baras, 2008. A lightweight certificate-based source authentication protocol for group communications in hybrid wireless-satellite networks. Proceedings of the 2008 IEEE Conference on Global Telecommunications (GLOBECOM '08), November 30-December 4, 2008, IEEE, New Orleans, Louisiana, ISBN:978-1-4244-2324-8, pp: 1-6.