ISSN 1392–124X INFORMATION TECHNOLOGY AND CONTROL, 2007 Vol. 36, No. 1, 1–5

A Key Agreement Scheme for Satellite Communications

Cheng-Chi Lee

Asia University, Department of Photonics and Communication Engineering
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.
E-mail: cclee@asia.edu.tw

Min-Shiang Hwang

National Chung Hsing University, Department of Management Information Systems
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
E-mail: mshwang@nchu.edu.tw
corresponding author

Tzu-Chun Lin

Feng Chia University, Department of Applied Mathematics
100 Wenhwa Rd, Seatwen, Taichung, Taiwan 407, R.O.C.

Abstract. Satellite communication technology was mainly used for broadcasting service and long-hual transmission. However, it is vulnerable to unauthorized access to the transmitted data. People are worried about two major security issues; privacy and authentication. Privacy refers to the guarantee that the communicated messages are not intercepted by an eavesdropper. On the other hand, authentication is carried out to ensure that any unauthorized user cannot fraudulently obtain his/her required services from the satellite communication systems. In this paper, the authors shall propose a new secure protocol based on key agreement scheme with mutual authentication to solve theses problems on the VSAT satellite communications. Compare with other key agreement schemes for VSAT satellite communications, our proposed scheme is more secure and efficient.

Key words: Authentication, DVB-RCS, key distribution, satellite communication, very small aperture terminal (VSAT).

1. Introduction

A satellite communication is an artificial satellite stationed in space for the purposes of telecommunications. Recent advances in satellite communication technology have a new thrust to use a low-cost very small aperture terminal (VSAT) network for data, voice, and video communications [4, 13, 20]. In general, a VSAT network is a star configuration including many VSATs and a single HUB. The HUB can communicate with the VSATs via the outbound links (HUB-to-VSAT) and a number of remote VSATs can communicate with the HUB via the inbound links (VSAT-to-HUB) [1, 14, 19]. The VSAT satellite communications have many advantages, such as high reliability, high quality of transmission, and low cost, at usage rates that are independent of distance, and simple network installation, operation, and management [2, 16]. In view of that, it is suitable for broadcasting service and long-hual transmission. However, it is vulnerable to unauthorized access to the transmitted data. People are worried about two major security issues; privacy and authentication [6, 8, 15]. Privacy refers to the guarantee that the communicated messages are not intercepted by an eavesdropper. On the other hand, authentication is carried out to ensure that any unauthorized user cannot fraudulently obtain his/her required services from the satellite communication systems.

To solve these security problems, it is critical to protect data communication in satellite communications by way of encryption and mutual authentication [7, 9–11]. In order to encrypt data exchanged between the HUB and the VSATs with secret key cryptosystems, a common secret key must be shared by them in advance. In 1998, Park and Lim [17] proposed key distribution schemes with mutual authentication to solve these security problems on the VSAT satellite communications. Unfortunately, Tseng [21] and Yi et al. [22], respectively, showed that Park-Lim schemes are insecure against an impersonation attack. Then, Tseng [21] proposed an improved scheme to remedy the impersonation attack and provided mutual authentication. In this paper, the authors shall propose a new secure protocol based on key agreement scheme with mutual authentication to solve theses security problems on the VSAT satellite communications. Compare with other key distribution schemes for VSAT satellite communications, our proposed scheme is more secure and efficient.

Recently, digital video broadcasting (DVB) return channel system (DVB-RCS) [12, 18] is the best known application of satellite technology, and was standardized by the European Telecommunications Standards Institute (ETSI) [5]. In general, a DVB-RCS network is a star configuration including many return channel satellite terminals (RCSTs) and a single network control center (NCC). The DVB-RCS security specification, currently supporting session key exchange between RCST and NCC, has three chosen schemes [3]. They are main key exchange scheme (MKE), quick key exchange scheme (QKE), and explicit key exchange scheme (EKE). QKE and EKE use a seed to derive a session key. MKE uses the Diffie-Hellman algorithm to derive a session key. However, these schemes are insecure. In QKE and EKE, an attacker can derive all the session keys if the attacker knows the seed. In MKE, an attacker can agree a session key between the RCST and the NCC. The architecture of DVB-RCS network is similar to VSAT network. Park-Lim [17], Yi et al. [22], and Tseng [21] have proposed VSAT-based key exchange schemes. However, their schemes are insecure. In this paper, the authors shall propose a new secure protocol based on key agreement scheme with mutual authentication to solve theses security problems on the VSAT satellite communications. Of course, our scheme can apply to DVB-RCS network.

The rest of this paper is organized as follows: In Section 2, we briefly review Tseng's scheme. In Section 3, we propose a new scheme. The security analysis and the performance analysis are described in Section 4. Finally, a summary is given in Section 5.

2. Review of Tseng's Scheme

In this section, we give a short description of Tseng's scheme. Tseng's scheme involves two phases: the initiation phase and the common key generation phase.

Initiation Phase: HUB is assigned to the key distribution center. The HUB generates two prime numbers p and q, and computes $N = p \cdot q$, chooses a random number d, and chooses a small prime e such that $e \cdot d \equiv 1 \bmod (p-1)(q-1)$. The HUB selects an integer g, which is the primitive element of both $GF(p)$ and $GF(q)$. The HUB calculates his/her secret key $S_h = {ID_h}^{-d} \bmod N$ and the VSAT's secret key $S_v = {ID_v}^{-d} \bmod N$. Then the HUB stores p, q, d and publishes N, g, e.

Common Key Generation Phase: HUB selects a random integer R_h, and then, computes $X_h = g^{R_h \cdot e} \bmod N$ and $Y_h = S_h \cdot g^{R_h \cdot h(X_h, ID_h, ID_v, t)} \bmod N$. VSAT randomly chooses a number R_v, and then calculates $X_v = g^{R_v \cdot e} \bmod N$ and $Y_v = S_v \cdot g^{R_v \cdot h(X_v, ID_v, ID_h, t)} \bmod N$ as well, where t is time stamp. After HUB and VSAT exchanging (X_h, Y_h) and (X_v, Y_v), HUB and VSAT compute the common key W_{hv} as $W_{hv} = (X_h)^{R_v} = (X_v)^{R_h} = g^{R_h \cdot R_v \cdot e} \bmod N$. Finally, HUB can check the validity of VSAT by checking whether the equation $ID_v = X_v^{h(X_v, ID_v, ID_h, t)} / (Y_v^e) \bmod N$ holds or not. In the same way, VSAT can check the validity of HUB by checking whether the equation $ID_h = X_h^{h(X_h, ID_h, ID_v, t)} / (Y_h^e) \bmod N$ holds or not. The above procedure is illustrated in Fig. 1.

3. Our Scheme

In this section, we propose our new scheme whose performance is much better than that of Tseng's scheme. There are also two phases in the proposed scheme: the initiation phase and the common key generation phase. The initiation phase in our scheme is the same as that of Tseng's scheme.

In common key generation phase, HUB selects a random number R_h, and then, computes X_h, S_v, and Y_h as follows:

$$\begin{aligned} X_h &= g^{R_h} \bmod N, \\ S_v &= {ID_v}^{-d} \bmod N, \\ Y_h &= h(X_h, h(S_v \oplus t)) \bmod N. \end{aligned}$$

Note that S_v may be pre-computed to reduce the computational cost. Thus, the HUB can store the VSAT's secret key S_v in his/her database. VSAT randomly chooses a number R_v, and calculates X_v and Y_v as follows:

$$\begin{aligned} X_v &= g^{R_v} \bmod N, \\ Y_v &= h(X_v, h(S_v \oplus t)) \bmod N. \end{aligned}$$

After HUB and VSAT exchanging (X_h, Y_h) and (X_v, Y_v), HUB can check the validity of VSAT by checking whether the following equation holds or not:

$$Y_v =? h(X_v, h(S_v \oplus t)) \bmod N.$$

If the above equation holds, HUB computes the common key $W_{hv} = (X_v)^{R_h} = g^{R_v R_h} \bmod N$. In the same way, VSAT can check the validity of HUB by checking whether the following equation holds or not:

$$Y_h =? h(X_h, h(S_v \oplus t)) \bmod N. \tag{1}$$

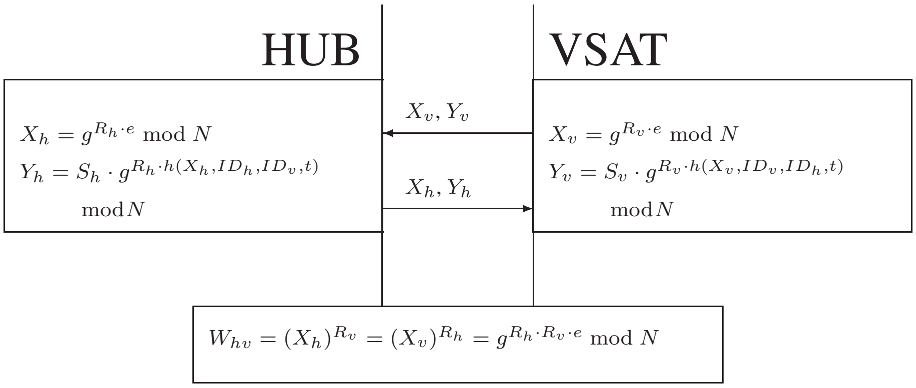

Fig. 1. Tseng's scheme

If the above equation holds, VSAT computes the common key $W_{hv} = (X_h)^{R_v} = g^{R_v R_h} \bmod N$. The above procedure is illustrated in Fig. 2.

In the following theorem, we show that the VSAT can authenticate the HUB. As the same reason, the HUB can also authenticate the VSAT. Thus, it can achieve mutual authentication.

Theorem 1. *Upon on receiving the message (X_h, Y_h), the VSAT can authenticate the HUB by checking whether the equation $Y_h = h(X_h, h(S_v \oplus t)) \bmod N$ holds.*

Proof. Since only the HUB has d, he/she can compute $S_v = ID_v{}^{-d} \bmod N$ and compute

$$Y_h = h(X_h, h(S_v \oplus t)) \bmod N.$$

Since the VSAT has S_v, it has

$$h(X_h, h(S_v \oplus t)) \bmod N.$$

Therefore, Y_h is equal to $h(X_h, h(S_v \oplus t)) \bmod N$. $\square$

4. Discussions

4.1. Security Analysis

In this section, we analyze the security of the proposed scheme. In the following, several possible attacks against our proposed scheme are presented.

Attack 1: An adversary tries the guessing attack.
Analysis of Attack 1: An adversary intercepts the (X_h, Y_h) and wants to guess the secret key S_v from the (X_h, Y_h). First, he/she chooses a value which is regarded as S_v' and check whether the equation 1 holds; if it shows that $S_v' = S_v$, then he/she finds the correct secret key S_v. Since it is difficult to directly find the secret key S_v, our scheme can resist the guessing attack.

Attack 2: An adversary tries the impersonation attack to forge the (X_h, Y_h).
Analysis of Attack 2: An adversary pretends that he/she is HUB and forges (X_h, Y_h). Firstly, he/she chooses a random number R_h and computes $X_h = g^{R_h} \bmod N$. Then, $Y_h = h(X_h, h(S_v' \oplus t))$ is computed and (X_h, Y_h) is sent to VSAT. After VSAT receives (X_h, Y_h), VSAT can check the validity of HUB by checking whether the equation $Y_h = h(X_h, h(S_v \oplus t))$ holds or not. Because the adversary does not have the secret key S_v and S_v is difficult to guess, VSAT will reject the adversary.

Attack 3: An adversary tries the replaying attack.
Analysis of Attack 3: An adversary intercepts the (X_h, Y_h) from HUB and stores it. After a while, he/she sends the (X_h, Y_h) to VSAT, and VSAT can check whether the equation $Y_h = h(X_h, h(S_v \oplus t'))$ holds or not. Because $Y_h = h(X_h, h(S_v \oplus t)), t \neq t'$, the equation $Y_h = h(X_h, h(S_v \oplus t'))$ is not held.

4.2. Performance Analysis

In the following, we show the performance of our proposed scheme. The performance evaluation of the proposed scheme mainly concerns the time complexity. For convenience, we suppose some notations are used to analyze the computational complexity as follows:

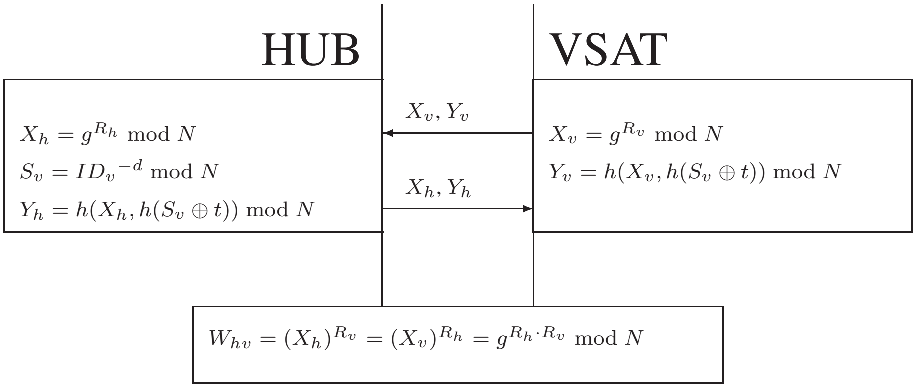

Fig. 2. Our scheme

- T_{exp} is the time for executing a modular exponentiation operation;
- T_h is the time for executing the one-way hash function $h(\cdot)$;
- T_{mul} is the time for modular multiplication.

Considering the computational complexity in the Park-Lim scheme with ID [17, 21], the total computational complexity required for the HUB is $7T_{exp} + 9T_{mul} + 2T_h$. And VSAT is needed to compute X_v, Y_v, and W_{hv}, of which the complexity is $8T_{exp} + 2T_{mul} + T_h$. The total complexity for the Park-Lim scheme with ID is $15T_{exp} + 11T_{mul} + 3T_h$ as shown in Table 1.

Tseng's scheme has a complexity of $5T_{exp} + 4T_{mul} + 2T_h$ for computing HUB, of which $T_{exp} + T_{mul}$, $T_{exp} + 2T_{mul} + T_h$, and T_{exp} are used to compute X_h, Y_h, and W_{hv}, respectively; in addition, $2T_{exp} + T_{mul} + T_h$ is required for checking whether the equation $ID_v = X_v^{h(X_v, ID_v, ID_h, t)}/(Y_v^e) \bmod N$ holds or not. Similarly, VSAT is needed to compute X_v, Y_v, and W_{hv}. They respectively require $T_{exp} + T_{mul}$, $T_{exp} + 2T_{mul} + T_h$, and T_{exp}. Meanwhile, the VSAT also needs to check whether the equation $ID_h = X_h^{h(X_h, ID_h, ID_v, t)}/(Y_h^e) \bmod N$ holds or not. It sums up to $2T_{exp} + T_{mul} + T_h$. Therefore, the total computational complexity required for the VSAT is $5T_{exp} + 4T_{mul} + 2T_h$. The total computational complexity required for the Tseng's scheme is $10T_{exp} + 8T_{mul} + 4T_h$ as shown in Table 1. Note that, in page 375 of [21], the total computational complexity required for the Tseng's scheme is stated as $10T_{exp} + 5T_{mul} + 3T_h$, which is not correct. It should be $10T_{exp} + 8T_{mul} + 4T_h$.

In our scheme, considering the computational complexity required for the HUB, the HUB is needed to compute X_h, Y_h S_v, and W_{hv}. Note that S_v may be pre-computed to reduce the computational cost. Thus, the HUB is only needed to compute X_h, Y_h, and W_{hv} on line. They respectively require T_{exp}, $2T_h$, and T_{exp}. Meanwhile, the HUB must check whether the equation $Y_v = h(X_v, h(S_v \oplus t)) \bmod N$ holds or not, which takes $2T_h$. Therefore, the total computational complexity required for the HUB is $2T_{exp} + 4T_h$. As for the complexity for the VSAT, the VSAT is needed to compute X_v, Y_v, and W_{hv}. They respectively require T_{exp}, $2T_h$, and T_{exp}; it also needs to check whether the equation $Y_h = h(X_h, h(S_v \oplus t)) \bmod N$ holds or not with the same cost of $2T_h$. Therefore, the total computational complexity required for the VSAT is $2T_{exp} + 4T_h$. Thus, the total computational complexity required for our scheme is $4T_{exp} + 8T_h$. Table 1 summarizes the comparison among Park-Lim scheme, Tseng's scheme, and our scheme. In conclusion, our scheme is more efficient than others.

5. Conclusions

In this paper, we have proposed a new secure key agreement scheme for VSAT satellite communications. The proposed scheme provides not only the secure key agreement but also mutual authentication. From Table 1, our scheme has the better performance than the Park-Lim scheme and Tseng's scheme in term of the computational complexity.

Acknowledgment

The authors would like to express their appreciation to the anonymous referees for their valuable suggestions and comments. This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the

Table 1. The comparison of three schemes in term of the computational complexity

	HUB	VSAT	Total
Park-Lim scheme with ID	$7T_{exp} + 9T_{mul} + 2T_h$	$8T_{exp} + 2T_{mul} + T_h$	$15T_{exp} + 11T_{mul} + 3T_h$
Tseng's scheme	$5T_{exp} + 4T_{mul} + 2T_h$	$5T_{exp} + 4T_{mul} + 2T_h$	$10T_{exp} + 8T_{mul} + 4T_h$
Our scheme	$2T_{exp} + 4T_h$	$2T_{exp} + 4T_h$	$4T_{exp} + 8T_h$

grant NSC96-2219-E-009-013 and NSC98-2221-E-468-002.

References

[1] N. Abramson, "VSAT data networks," *Proceedings of the IEEE*, vol. 78, pp. 1267–1274, July 1990.

[2] D. M. Chitre and J. S. McCoskey, "VSAT networks: architectures, protocols, and management," *IEEE Communications Magazine*, vol. 26, no. 7, pp. 28–38, 1988.

[3] H. Cruickshank, M. P. Howarth, S. Iyengar, Zhili Sun, and L. Claverotte, "Securing multicast in DVB-RCS satellite systems," *IEEE Wireless Communications*, vol. 12, no. 5, pp. 38–45, 2005.

[4] V. M. Dorofeev and L. Y. Kantor, "VSAT applications in Russian satellite communications," *International Journal of Satellite Communications*, vol. 11, no. 4, pp. 223–228, 1993.

[5] ETSI, "Digital video broadcasting (DVB); interaction channel for satellite distribution systems," *ETSI EN 301 790 v. 1.3.1*, Mar. 2003.

[6] K. F. Hwang and C. C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Transactions on Wireless Communications*, vol. 2, no. 2, pp. 400–407, 2003.

[7] M. S. Hwang and W. P. Yang, "Conference key distribution schemes for secure digital mobile communications," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 2, pp. 416–420, Feb. 1995.

[8] Min-Shiang Hwang, "Dynamic participation in a secure conference scheme for mobile communications," *IEEE Transactions on Vehicular Technology*, vol. 48, no. 5, pp. 1469–1474, 1999.

[9] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, 2006.

[10] C. C. Lee, M. S. Hwang, and W. P. Yang, "Extension of authentication protocol for GSM," *IEE Proc.-Communication*, vol. 150, no. 2, pp. 91–95, 2003.

[11] W. B. Lee and C. K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," *IEEE Transactions on Wireless Communications*, vol. 4, no. 1, pp. 57–64, 2005.

[12] Ricardo Castellot Lou, Antonio Javier Sanchez Esguevillas, Borja de la Cuesta Diego, Belen Carro, Linghang Fan, and Zhili Sun, "IPv6 networks over DVB-RCS satellite systems," *International Journal of Satellite Communications and Networking*, vol. 26, no. 1, pp. 45–56, 2008.

[13] M. Maggenti, T. T. Ha, and T. Pratt, "VSAT Networks - an overview," *International Journal of Satellite Communications*, vol. 5, no. 3, pp. 219–225, 1987.

[14] Michael W. Mitchell and Robert A. Hedinger, "The development of VSAT performance standards in the United States of America," *International Journal of Satellite Communications*, vol. 11, no. 4, pp. 195–200, 1993.

[15] S. Mohan, "Privacy and authentication protocols for PCS," *IEEE Personal Communications*, vol. 3, no. 5, pp. 34–38, Oct. 1996.

[16] K.M.S. Murthy, J. Alan, J. Barry, B.G. Evans, N. Miller, R. Mullinax, P. Noble, B. O'Neal, J.J. Sanchez, N. Seshagiri, D. Shanley, J. Stratigos, and J.W. Warner, "VSAT user network examples," *IEEE Communications Magazine*, vol. 27, no. 5, pp. 50–57, 1989.

[17] Jeong-Hyun Park and Sun-Bae Lim, "Key distribution for secure VSAT satellite communications," *IEEE Transactions on Broadcasting*, vol. 44, no. 3, pp. 274–277, 1998.

[18] Dionysia K. Petraki, Markos P. Anastasopoulos, and Panayotis G. Cottis, "Dynamic resource allocation for DVB-RCS networks," *International Journal of Satellite Communications and Networking*, vol. 26, no. 3, pp. 189–210, 2008.

[19] A. H. Rana, J. S. McCoskey, and W. A. Check, "VSAT technology, trends, and applications," *Proceedings of the IEEE*, vol. 78, pp. 1087–1095, July 1990.

[20] L. P. Seidman, "Satellite for wideband access," *IEEE Communications Magazine*, vol. 34, no. 10, pp. 108–111, Oct. 1996.

[21] Y. M. Tseng, "Cryptanalysis and improvement of key distribution system for VSAT satellite communications," *Informatica*, vol. 13, no. 3, pp. 369–376, 2002.

[22] Xun Yi, Chee Kheong Siew, Hung-Min Sun, Her-Tyan Yeh, Chun-Li Lin, and Tzonelih Hwang, "Security of Park-Lim key agreement schemes for VSAT satellite communications," *IEEE Transactions on Vehicular Technology*, vol. 52, no. 2, pp. 465–468, March 2003.