INFORMATICA, 2002, Vol. 13, No. 3, 369–376

Cryptanalysis and Improvement of Key Distribution System for VSAT Satellite Communications *

Yuh-Min TSENG
Department of Information Management, Nan-Kai College
Nantou, Taiwan 542, R.O.C.
e-mail: tym@nkc.edu.tw

Received: June 2002

Abstract. Recently, Park and Lim (1998) proposed two key distribution systems for secure VSAT satellite communications. One provides indirect authentication, and another scheme enables that two parties can directly authenticate each other. However, this article will show that the proposed schemes are insecure enough by presenting two impersonation attacks on them. Besides, an improved scheme will be proposed, which is secure against the impersonation attack and provides direct mutual authentication between two parties.

Key words: satellite communication, key distribution, cryptanalysis.

1. Introduction

Satellite communications have been implemented for many systems. A main characteristic of satellite communications is that they provide wireless access to traditional wire-line networks for a large number of access services. In recent years, satellite data communications using VSATs (Very Small Aperture Terminal) is extending to more and more services for maritime, aeronautical, and land systems. Most VSAT networks use a star configuration, which composes a single HUB communicating with remote VSATs. The VSAT satellite communications have many advantages, such as high reliability and quality of communications, low cost and flat usage rates independent of distance, simple network installation (Chitre and Mccoskey, 1988; Murthy, 1989).

However, wireless transmission is vulnerable to relatively easy interception, such as fraudulent call attempts and intrusion by an unauthorized user (Hall and Maher, 1993). Therefore, we must consider the security of transmitted data, and a feasible solution for implementation of secure VSAT satellite communications is needed. Privacy and authentication must be considered. Privacy involves ensuring an eavesdropper cannot intercept data communications. Authentication confirms legal identities to avoid any vicious impostor and ensures that services are not obtained fraudulently in order to avoid charges for usage.

* This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no. NSC89-2213-E-252-008.

Recently, Park and Lim (1998) described a security protocol based on key distribution schemes to solve security problems on VSAT networks. They first presented a key distribution system using the modified Diffie–Hellman scheme (Diffie and Hellman, 1976), which provides the indirect authentication. Then they described another scheme based on the modified Diffie–Hellman scheme with ID, which is able to defend the network from imposters and enables that two parties can directly authenticate each other.

Unfortunately, this article will show that the Park–Lim schemes are insecure enough by presenting two impersonation attacks. According to the attacks, any malicious attacker without knowing any secret key can impersonate a legal VSAT or HUB to communicate with HUB and VSAT. Moreover, an improved scheme will be proposed that enables two parties to hold a secure common key and provides the mutually direct authentication between two parties. Certainly, the secure requirement against the impersonation attack will also be concerned about.

2. Cryptanalysis of Park–Lim Key Distribution Schemes

In this section, we will show that two schemes proposed by Park and Lim are not secure enough by presenting two impersonation attacks. For presenting our attacks on Park–Lim schemes, we briefly review their schemes along with our attacks.

Two key distribution schemes for secure VSAT satellite communications were proposed by Park and Lim. One is based on the modified Diffie–Hellman scheme, which provides indirect authentication between HUB and VSAT. Another scheme uses the modified Diffie–Hellman scheme with ID to enable that HUB and VSAT can directly authenticate each other. In their schemes, HUB is assigned to the key distribution center. Both schemes have the same initiation phase, the parameters are presented as follows: the HUB selects two large prime numbers p and q, and selects a prime number e and an integer d that satisfy $N = p \cdot q$ and $e \cdot d \equiv 1 \bmod (p-1)(q-1)$. The HUB also chooses an integer g which is a primitive element over $GF(p)$ and $GF(q)$. The HUB with identity ID_h generates his secret key $S_h = ID_h^{-d} \bmod N$ and the VSAT's secret key $S_v = ID_v^{-d} \bmod N$. The HUB keeps p, q and d secret and publishes N, g and e to all VSATs. In the following subsection, we review the common key generation phase of their two schemes and present our attacks.

2.1. *Adaptation of the Modified Diffie–Hellman Scheme*

The following is the adaptation procedure of the modified Diffie–Hellman scheme for VSAT satellite communications.

Step 1. HUB computes his public key $P_h = g^{S_h} \bmod N$ and VSAT's public key $P_v = g^{S_v} \bmod N$.

Step 2. HUB chooses a random numbers R_h, and computes $X_h = g^{R_h} \bmod N$ and $Y_h = X_h \cdot Z_{hv} \bmod N$, where $Z_{hv} = P_v^{S_h} = P_h^{S_v} = g^{S_h S_v} \bmod N$. Similarly, VSAT also generates R_v, X_v and Y_v. Then HUB and VSAT exchange (X_h, Y_h) and (X_v, Y_v).

Step 3. HUB and VSAT compute the common key W_{hv} as

$$W_{hv} = (Y_v \cdot Z_{hv}^{-1})^{R_h} = (Y_h \cdot Z_{hv}^{-1})^{R_v} = g^{R_h R_v} \bmod N.$$

As we can see that the computation of the common key W_{hv} needs the secret session key Z_{hv} only known for HUB and VSAT. So it provides indirect authentication between HUB and VSAT.

[*Attack 1*]

The first attack concerns on the key distribution based on the modified Diffie–Hellman scheme. An impostor can easy obtain (X_h, Y_h) and (X_v, Y_v), which were previously exchanged for establishing the common key between HUB and VSAT. Therefore, an impostor can compute $Z_{hv} = Y_h \cdot X_h^{-1} \bmod N = Y_v \cdot X_v^{-1} \bmod N$, where Z_{hv} is the secret session key shared with HUB and VSAT. Since the impostor knows Z_{hv}, he can impersonate the VSAT to perform the common key exchange procedure with HUB. Similarly, he may also impersonate HUB to establish the communication with the VSAT.

2.2. *Adaptation of the Modified Diffie–Hellman Scheme with ID*

The key distribution using the modified Diffie–Hellman scheme with ID is presented as follows.

Step 1. HUB chooses a random number R_h, and computes $X_h = g^{R_h S_h + ID_v} \bmod N$. VSAT also generates R_v and compute $X_v = g^{R_v S_v + ID_h} \bmod N$. Then HUB and VSAT exchange X_h and X_v.

Step 2. HUB and VSAT first compute $C_h = hash(X_h, ID_h, ID_v, t)$ and $C_v = hash(X_v, ID_v, ID_h, t)$, where t is time stamp. Then HUB and VSAT compute $Y_h = g^{R_h S_h C_h} \bmod N$ and $Y_v = g^{R_v S_v C_v} \bmod N$, respectively. Then HUB and VSAT exchange Y_h and Y_v.

Step 3. HUB and VSAT compute the common key W_{hv} as

$$W_{hv} = (g^{-ID_v} \cdot X_h)^{R_v S_v} = (g^{-ID_h} \cdot X_v)^{R_h S_h} = g^{R_h R_v S_h S_v} \bmod N.$$

Step 4. Meanwhile, HUB can authenticate the VSAT by checking whether the following equation holds or not.

$$S_v = X_h^{C'_h} / (Y_h \cdot g^{ID_v C_h} \cdot ID_v^d) \bmod N.$$

If X_h is modified, C'_h is not equal to C_h. However, it can be seen that Step 4 in the above scheme, the checking equation always holds because $X_h^{C'_h} = Y_h \cdot g^{ID_v C_h} \bmod N$ and $S_v = ID_v^{-d} \bmod N$. That is, it can not provide direct authentication. In such way, the impersonation attack is presented as follows.

[*Attack 2*]

In the following, an example is given to describe the impersonation attack. HUB will believe that the impostor is the VSAT with identity ID_v after performing the following procedure:

Step 1. HUB chooses a random number R_h, and computes $X_h = g^{R_h S_h + ID_v} \bmod N$. The impostor randomly chooses two integers R_a and S_a, and compute $X_v = g^{R_a S_a + ID_h} \bmod N$. Then HUB and the impostor exchange X_h and X_v.

Step 2. HUB and the impostor compute $C_h = hash(X_h, ID_h, ID_v, t)$ and $C_v = hash(X_v, ID_v, ID_h, t)$, where t is time stamp. Then HUB and the impostor compute $Y_h = g^{R_h S_h C_h} \bmod N$ and $Y_v = g^{R_a S_a C_v} \bmod N$, respectively. Then HUB and the impostor exchange Y_h and Y_v.

Step 3. HUB and the impostor compute the common key W_{hv} as

$$W_{hv} = (g^{-ID_v} \cdot X_h)^{R_a S_a} = (g^{-ID_h} \cdot X_v)^{R_h S_h} = g^{R_h R_a S_h S_a} \bmod N.$$

Step 4. Meanwhile, HUB and the impostor can authenticate each other by checking whether the following equations hold or not.

$$S_v = X_h^{C'_h} / (Y_h \cdot g^{ID_v C_h} \cdot ID_v^d) \bmod N.$$

From the above descriptions, it can be seen that the impostor can use the common key $W_{hv} = g^{R_h R_a S_h S_a} \bmod N$ to communicate with HUB, and HUB believes that the impostor is the VSAT with identity ID_v. Therefore, this impersonation attack is successful.

3. The Improved Scheme

Here, a secure key distribution scheme for VSAT satellite communications will be proposed. It employs the concept of digital signature to achieve the direct authentication. Initially, HUB is assigned to the key distribution center. The HUB selects two prime numbers p and q, and selects a small prime number e(e.g. $e = 3$) such that $e \cdot d \equiv 1 \bmod (p-1)(q-1)$. The HUB also chooses an integer g which is a primitive element over $GF(p)$ and $GF(q)$. The HUB with identity ID_h computes his secret key $S_h = ID_h^{-d} \bmod N$ and the VSAT's secret key $S_v = ID_v^{-d} \bmod N$. The HUB keeps p, q and d secret and publishes $N = p \cdot q, g$ and e to all VSATs. The key distribution scheme with direct mutual authentication for VSAT satellite communications is presented as follows.

Step 1. HUB chooses a random number R_h, and computes $X_h = g^{R_h \cdot e} \bmod N$ and $Y_h = S_h \cdot g^{R_h \cdot h(X_h, ID_h, ID_v, t)} \bmod N$, where t is time stamp. Similarly, VSAT also generates R_v and computes $X_v = g^{R_v \cdot e} \bmod N$ and $Y_v = S_v \cdot g^{R_v \cdot h(X_v, ID_v, ID_h, t)} \bmod N$. Then HUB and VSAT exchange (X_h, Y_h) and (X_v, Y_v).

Step 2. HUB and VSAT compute the common key W_{hv} as

$$W_{hv} = (X_h)^{R_v} = (X_v)^{R_h} = g^{R_h R_v e} \bmod N.$$

Step 3. Meanwhile, HUB can authenticate the VSAT by checking whether the following equation hold or not.

$$ID_v = X_v^{h(X_v, ID_v, ID_h, t)} / (Y_v^e) \bmod N.$$

Note that if the VSAT wants to authenticate the HUB, he also check whether the following equation $ID_h = X_h^{h(X_h, ID_h, ID_v, t)} / (Y_h^e) \bmod N$ hold or not.

In the following theorem, we show that the VSAT can authenticate the HUB. As the same reason, the HUB can also authenticate the VSAT.

Theorem. *Upon on receiving the messages* (X_h, Y_h)*, the VSAT can authenticate the HUB by checking whether the equation* $ID_h = X_h^{h(X_h, ID_h, ID_v, t)} / (Y_h^e) \bmod N$ *holds.*

Proof. Since $X_h = g^{R_h \cdot e} \bmod N$ and $Y_h = S_h \cdot g^{R_h \cdot h(X_h, ID_h, ID_v, t)} \bmod N$ and, we have

$$\begin{aligned} & X_h^{h(X_h, ID_h, ID_v, t)} / (Y_h^e) \bmod N \\ & \quad = (g^{R_h e})^{h(X_h, ID_h, ID_v, t)} / (S_h \cdot g^{R_h \cdot h(X_h, ID_h \cdot ID_v, t)})^e \bmod N \\ & \quad = 1 / S_h^e \bmod N = S_h^{-e} \bmod N. \end{aligned}$$

Because of the HUB's secret key $S_h = ID_h^{-d} \bmod N$, and multiplying the equation by a number $-e$, we have the equation $S_h^{-e} = ID_h^{ed} \bmod N$. And $e \cdot d \equiv 1 \bmod (p-1)(q-1)$ as the RSA scheme (*Rivest et al.*, 1978), so $S_h^{-e} = ID_h \bmod N$.

4. Discussions and Comparisons

In the improved scheme, assume that an opponent wants to impersonate a legal VSAT with identity ID_v to communicate with HUB. He must calculate $X'_v = g^{R_v \cdot e} \bmod N$ and $Y'_v = (ID_v)^{-d} \cdot g^{R_v \cdot h(X'_v, ID_v, ID_h, t)} \bmod N$ such that $ID_v = X'^{\,h(X'_v, ID_v, ID_h, t)}_v / (Y'^{\,e}_v) \bmod N$ can be checked correct. However, to compute $(ID_v)^{-d}$ is equivalent to breaking the RSA scheme (Rivest *et al.*, 1978). Therefore, the proposed scheme ensures that an impostor cannot impersonate a legal VSAT. The proposed scheme really has direct mutual authentication between HUB and VSAT. It is seen by checking the correctness of ID at Step 3 of the proposed scheme.

In the following, the comparisons between the improved scheme and Park–Lim scheme with ID are given for the viewpoint of the computational complexity as well as transmission efficiency. The performance evaluation of the improved scheme includes

the total bit length of transmitted messages, and the computational complexity needed for the HUB and the VSAT. For convenience, the following notations are used to analyze the performance. $|Z|$ is the bit length of Z; T_{mul} is the time for modular multiplication; $T_{\exp}$ is the time for modular exponentiation; T_h is the time of executing the hash function algorithm $hash$. Note that the time for computing modular addition is ignored, because it is much smaller than T_{mul}, $T_{\exp}$ and T_h.

As for the computational complexity and the communication cost in the Park–Lim scheme with ID, the transmitted messages are (X_v, Y_v, X_h, Y_h). The communication cost is $4|N|$. Considering the computational complexity required for the HUB, the HUB is needed to compute X_h, Y_h and W_{hv}. They respectively require $T_{\exp} + T_{mul}, T_{\exp} + 2T_{mul} + T_h$ and $T_{\exp} + 2T_{mul}$. For example, computing $X_h = g^{R_h S_h + ID_v} \bmod N$, the HUB first compute a temporary value $Temp = R_h S_h + ID_v \bmod (p-1)(q-1)$ because he knows the components p and q of N, then computes $X_h = g^{Temp} \bmod N$. In such case, it requires $T_{\exp} + T_{mul}$. Meanwhile, the HUB must check whether the equation $S_v = X_h^{C'_h}/(Y_h \cdot g^{ID_v C_h} \cdot ID_v^d) \bmod N$ holds or not. It requires $4T_{\exp} + 4T_{mul} + T_h$. Therefore, the total computational complexity required for the HUB is $7T_{\exp} + 9T_{mul} + 2T_h$. As for considering the computational complexity required for the VSAT, the VSAT is needed to compute X_v, Y_v and W_{hv}. Note that the components p and q of N are unknown to the VSAT, so he can not compute the exponential part of X_v and Y_v using $(p-1)(q-1)$ in advance. They respectively require $3T_{\exp} + T_{mul}, 3T_{\exp} + T_h$ and $2T_{\exp} + T_{mul}$. Therefore, the total computational complexity required for the VSAT is $8T_{\exp} + 2T_{mul} + T_h$.

In our improved scheme, the transmitted messages are also (X_v, Y_v, X_h, Y_h). The communication cost is $4|N|$. Considering the computational complexity required for the HUB, the HUB is needed to compute X_h, Y_h and W_{hv}. They respectively require $T_{\exp} + T_{mul}, T_{\exp} + 2T_{mul} + T_h$ and $T_{\exp}$. Meanwhile, the HUB must check whether the equation $ID_v = X_v^{h(X_v, ID_v, ID_h, t)}/(Y_v^e) \bmod N$ holds or not. It requires $2T_{\exp} + T_{mul} + T_h$. Therefore, the total computational complexity required for the HUB is $5T_{\exp} + 4T_{mul} + 2T_h$. As for considering the computational complexity required for the VSAT, the VSAT is needed to compute X_v, Y_v and W_{hv}. They respectively require $2T_{\exp}, 2T_{\exp} + T_{mul} + T_h$ and $T_{\exp}$. Therefore, the total computational complexity required for the VSAT is $5T_{\exp} + T_{mul} + T_h$.

Comparisons for the total bit length of transmitted messages and the computational complexity between the Park–Lim scheme with ID and our improved scheme are summarised in Table 1. Therefore, our improved scheme has the better performance in term of the computational complexity. Moreover, in the Park–Lim scheme with ID, they have the simulation result of 512 bits on PC 486 using MD5 (Rivest, 1992) for hash function and Montgomery (Montgomery, 1993) for modular. Their result is reasonable to VSAT satellite communications, which requires about 200–600 ms for delay time. Certainly, the improved scheme is also suitable to be implemented on VSAT satellite communications.

Table 1
Comparison between our improved scheme and the Park–Lim scheme with ID

	The Park–Lim scheme with ID	Our improved scheme
The bit-length of transmitted messages	$4\|N\|$	$4\|N\|$
Computational complexity required for the HUB	$7T_{\exp} + 9T_{mul} + 2T_h$	$5T_{\exp} + 4T_{mul} + 2T_h$
Computational complexity required for the VSAT	$8T_{\exp} + 2T_{mul} + T_h$	$5T_{\exp} + T_{mul} + T_h$

5. Conclusions

It has been showed that the Park–Lim schemes are not secure by presenting impersonation attacks on them. According to the presented attacks, any malicious attacker without knowing any secret key can impersonate a legal VSAT or HUB to communicate with HUB and VSAT. Besides, an improved scheme has been proposed. The improved scheme provides not only the secure key distribution but also mutual authentication. The new scheme is secure against the impersonation attack. From Table 1, we know that our improved scheme has the better performance than the Park–Lim scheme in term of the computational complexity.

Acknowledgements

The authors would like to thank the referees for their valuable and constructive suggestions.

References

Chitre, D.M., J.S. Mccoskey (1988). VSAT networks: architectures, protocol, and management. *IEEE Communication Magazine*, **26**(7), 28–38.

Diffie, W., M.E. Hellman (1976). New directions in cryptography. *IEEE Trans. on Infomation Theory*, **22**(6), 644–654.

Hall, S.R., D.P. Maher (1993). Closing in on wireless privacy. *AT&T Technology*, **8**(3), 22–25.

Montgomery, P.L. (1993). Modular multiplication algorithm using lookahead determination. *IEICE Trans.*, **E76-A**(1), 70–77.

Murthy, K.M. (1989). VSAT user network examples. *IEEE Communication Magazine*, 50–57.

Park, J.H., S.B. Lim (1998). Key distribution for secure VSAT satellite communications. *IEEE Trans. on Broadcasting*, **44**(3), 274–277.

Rivest, R.L. (1992). The MD5 message digest algorithm. *Requests for Comments (RFC) 1321*.

Rivest, R.L., A. Shamir, L. Adelman (1978). A method for obtaining digital signature and public key cryptosystem. *Commun. ACM*, **21**(2), 120–126.

Y.-M. Tseng received the B.S. degree in Computer Science and Engineering from National Chiao Tung University, Taiwan, Republic of China, in 1988; and the M.S. degree in Computer and Information Engineering from National Taiwan University in 1990, and the Ph.D. in Applied Mathematics from National Chung Hsing University in 1999. He is currently an Associate Professor and the chairman of the Department of Information Management, Nan-Kai College, Taiwan. He is a member of the Chinese Association for Information Security (CCISA). His research interests include cryptography, mobile communication security, network security, and image encryption.

Kryptoanalizė ir rakto paskirstymo sistemos tobulinimas VSAR palydoviniams ryšiams

Yuh-Min TSENG

Park ir Lim (1998) pasiūlė dvi rakto paskirstymo sistemas saugiems VSAT palydoviniams ryšiams. Viena sistema leidžia netiesioginę autentizaciją. Kita leidžia abiems komunikuojančioms pusėms tiesiogiai autentizuoti vienai kitą. Šis straipsnis parodo, kad abi pasiūlytos schemos nėra pakankamai saugios. Taip pat pasiūlyta saugesnė schema, leidžianti tiesioginį abipusį autentizavimą tarp abiejų pusių.