Efficiency Evaluation for Key Distribution Models in Satellite Terminals*

Taeshik Shon[1], Jongsub Moon[1], and HongMin Choi[2]

[1] Center for Information Security Technologies, Korea University, Seoul, Korea
{743zh2k,jsmoon}@korea.ac.kr
[2] Information Security Technology Institute, Secuve Co.Ltd,., Seoul, Korea
partout@secuve.com

Abstract. With the increasing use of satellite communications, there is growing concern, regarding security problems. These problems are caused by characteristics such as providing world wide coverage with distance-insensitive cost, large transmission bandwidth, and so on. In this paper we propose four kinds of key distribution models to achieve information security between satellite terminals. Also, through performance analysis of proposed models, we verify their suitability to satellite environments.

Keywords : key distribution, satellite security, performance evaluation

1 Introduction

With the development of communication technology, users want excellent information communication services provided at high speed, wide bandwidth, multimedia capability and mobility. Satellite communication can be used to fulfill such requirements. Thus, it is important to establish a secure communication channel among satellite terminals according to the rising demand of satellite communication. In this paper, we propose four kinds of key distribution models, and verify them. The paper is composed as follows: Section 1 introduces the overview of satellite security. Section 2 studies the considerations of key distribution models with push/pull scheme. Section 3 proposes four kinds of key distribution models in satellite environments. Section 4 verifies performance in these environment. Finally, Section 5 concludes this paper.

2 Previous Work

Key distribution procedure can be classified into the Push and Pull models in accordance with how to get a secret key. In the Push-typed model(as illustrated in Figure 1), user A generates the secret key for secure channel establishment between users, and then transfers the generated secret key to a corresponding B

* This work was supported (in part) by the Ministry of Information&Communications, Korea, under the Information Technology Research Center (ITRC) Support Program

after the authentication process of the security server. Such a Push model needs three times message exchanges for the secret key distribution as follows: User A requests authentication to the security server (i), the security server sends user A a encrypted message used between server and user B as a session key(ii), and finally A distributes the message to B. In the Pull typed key distribution model, User A requests authentication and key distribution to the security server, and then the security server distributes the secret key to each user. In such a Pull model, twice message exchanges are enough for the secret key distribution because this scheme transfers the secret key to each user from security server at the same time[1–4].

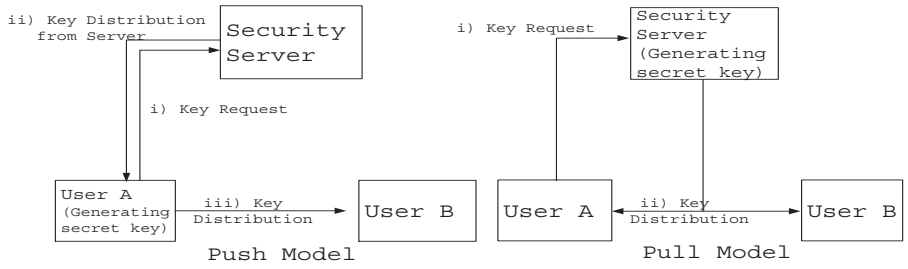

Fig. 1. Push and Pull-typed Key Distribution Models

3 Four types of Key Distribution Models

Because satellite networks is affected by propagation delay caused by environmental characteristic, key distribution models must consider round trip delay (max:278msec, min:238msec). Thus, we must satisfy the requirement that simplifies key distribution procedure among terminals. Also, we must consider the processing speed of algorithm used to accomplish authentication, encryption and minimization of message sizes which is transmitted to other terminals.

Table 1. Combining between key distributions models and Encryption algorithms

Encryption Algorithm / Key Distribution Model	Symmetric Key Encryption	Public Key Encryption
Push	Case 1	Case 2
Pull	Case 3	Case 4

3.1 Push typed key distribution models (Case 1, Case2)

Push typed model with symmetric key encryption (Case 1):

1. TA sends own ID_A and encrypted message including ID_B , Timestamp and the secret key between A and B to SS
2. If TA is authenticated, SS sends encrypted message including ID_A, Timestamp and the secret key to TA.
3. TA sends encrypted message including ID_A and the secret key to B.

1. $TA \rightarrow SS : ID_A||E_{AS}[ID_B||K_{AB}||T]$
2. $SS \rightarrow TA : E_{BS}[ID_A||K_{AB}||T]$
3. $TA \rightarrow TB : E_{BS}[ID_A||K_{AB}]$

Table 2. Notations of Symmetric key algorithm

Notations	Description
SS	Satellite Security Server
TA, TB	Terminal A, Terminal B
K_{AB}	Secret key between A and B
E_{AB}	Encryption using secret key between A and B
E_{KUx}/E_{KRx}	Public key and Private key of X
$Sign_{KRx}()$	Sign value with private key of x
T	Timestamp
ID_X	Identification of Terminal X

Push typed model with public key encryption algorithm(Case 2):

1. TA requests communication to SS through satellite. And, TA sends encrypted message with ID of Terminal A, B and the secret key to SS. In this time, the secret key is generated by TA.
2. SS sends encrypted message to TA. This message comprised as follows: Encrypted with public key of TB together with signature to message (m_2) which is comprised with identity of TA, secret key between TA and TB, and timestamp.
3. TA sends this encrypted message to TB.

1. $TA \rightarrow SS : E_{KUss}[m_1||Sign_{KUa}(m_1)]$
2. $SS \rightarrow TA : E_{KUb}[m_2||Sign_{KRss}(m_2)]$
3. $TA \rightarrow TB : E_{KUb}[m_2||Sign_{KRss}(m_2)]$

$*m_1 = (ID_A||ID_B||K_{AB}), m_2 = (ID_B||K_{AB}||T)$

3.2 Pull typed key distribution models (Case 3, Case4)

Pull typed model using symmetric key encryption algorithm(Case 3):

1. TA sends own ID_A and encrypted message including ID_B and timestamp to SS.

2. If TA is authenticated, SS sends encrypted message including ID_B and the secret key to TA. Also, SS sends encrypted message including ID_A , timestamp and the secret key to TB. In this procedure, the secret key for secure channel is generated by SS.

1. $TA \rightarrow SS : E_{AS}[ID_A||ID_B||T]$
2. $SS \rightarrow TA : E_{AS}[ID_B||K_{AB}||T]$
   $SS \rightarrow TB : E_{BS}[ID_A||K_{AB}||T]$

Pull typed model using public key encryption algorithm(Case 4):

1. TA requests communication to SS through satellite. At this time, TA sends encrypted message with ID of Terminal A, B to SS.
2. SS sends encrypted message to TA. This message comprised as follows: Encrypted with public key of A together with signature to message (m_2) which is comprised with identity of A, secret key between TA and TB, and timestamp. Also SS sends encrypted message(m_3) to TB. In this procedure, the secret key for secure channel is generated by SS.

1. $TA \rightarrow SS : E_{KUa}[m_1||Sign_{KUa}(m_1)]$
2. $SS \rightarrow TA : E_{KUa}[m_2||Sign_{KRss}(m_2)]$
   $SS \rightarrow TB : E_{KUb}[m_3||Sign_{KRss}(m_3)]$
   $*m_1 = (ID_A||ID_B), m_2 = (ID_A||K_{AB}||T), m_3 = (ID_B||K_{AB}||T)$

4 Performance Analysis

4.1 Experimental Methods

Fig. 2. Modeling of satellite communication systems

This section analyzes suitability of the proposed four kinds of key distribution models for satellite networks. To analyze suitability of proposed models, we calculate the sum of delay time related to some parameters such as encryption algorithm, distributed key length. We make model of satellite communication systems, as illustrated in Figure 2. It consists of satellite(SAT), satellite mobile terminals(MT) and satellite security server(SS). Our model of satellite systems referred to the security service modeling of normal data communication and included the characteristic of satellite networks[5–8]. Table 3 indicates each parameters of model for satellite systems. We assume that packets arrive according

to poisson distribution with arrival rate λ and service times have constant values such as μ_1, μ_2 and μ_3. Even if we consider additional information security services to each system such as encryption, decryption, signature and verification, arrival rate is maintained equally, but service rate is added by μ_1', μ_2' and μ_3' respectively. The best efficiency of this systems is $\mu_b' = \max(1/\mu_i')$,i=1,2,3, that is, it is determined by system which has the longest service time. The average delay time of system is same as the sum of the spent time in each system queue. In modeling satellite systems, because we assume additionally the information security service to normal satellite systems, the service time of each system has additional deterministic service time (information security service). As according to the addition of information security service, the service time of each system also increases deterministically. Thus, among the queuing models, we made modeled satellite systems which provide information security service with an M/D/1 queuing model and derived an equation to calculate the delay time of total systems as follows.

$$\rho_i = \lambda/\mu_i,\ d_i = \mu_i/\mu_i'(\mu_i' = \mu_i/d_i) \tag{1}$$

$$\rho_i' = \lambda/\mu_i' = \lambda * d_i/\mu_i = d_i * \lambda/\mu_i = d_i * \rho_i \tag{2}$$

In equation (3), T is total delay and we can find it from w(M/D/1 queue's average delay time $\mu^{-1} + \rho\mu^{-1}/2(1-\rho)$) plus all systems delay time($\sum_{i=1,i\neq b}^{3} \frac{1}{\mu_i'}$) plus satellite propagation delay(ld*2).

$$T = w + \sum_{i=1,i\neq b}^{3} \frac{1}{\mu_i'} + (ld * 2), (\mu_b' = max[1/\mu_i']_{,i=1,2,3}) \tag{3}$$

$$= (1/\mu_b' + \rho_b'\mu_b^{-1}/2(1-\rho_b')) + \sum_{i=1,i\neq b}^{3} \frac{1}{\mu_i'} + (ld * 2) \tag{4}$$

$$= \rho_b'\mu_b^{-1}/2(1-\rho_b') + \sum_{i=1}^{3} \frac{1}{\mu_i'} + (ld * 2) \tag{5}$$

$$= \lambda/2\mu_b'(\mu_b' - \lambda) + \sum_{i=1}^{3} \frac{1}{\mu_i'} + (ld * 2) \tag{6}$$

In equation (6), we derived the total delay time of satellite systems.

All encryption algorithms were coded in C++ or ported to C++ from C implementations, compiled with Microsoft Visual C++ 6.0 SP4 (optimize for speed, blend code generation), and ran on a Celeron 850MHz processor under Windows 2000 SP 1(As illustrated Table 4, Table 5)[9]. Also we assumed that basic delay time of satellite communication systems and other systems is 0.01msec, round trip delay time between satellite and terminals is 250msec(that is, ld=125msec) and arrival rate is 10 packets/slot.

Table 3. Notations of Modeling of Satellite Communication Systems

Notations	Description
ρ_i	Efficiency of normal systems
ρ_i'	Efficiency of information security systems
μ_i	Service rate of normal systems
μ_i'	Service rate of Information security systems
λ	Arrival rate
d_i	Differentiation between service rate of normal systems and service rate of information security systems
T	Total Delay
L_d	Delay time of satellite link

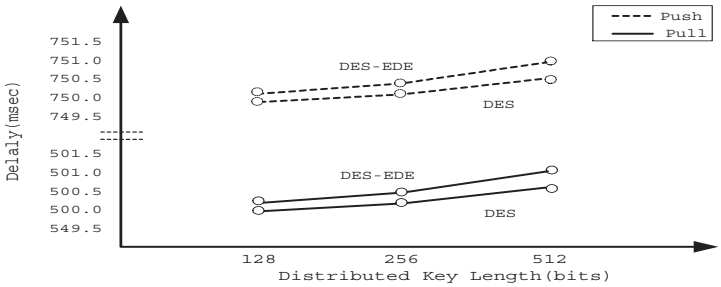

Fig. 3. Delay Comparison using Symmetric key encryption algorithms(Case1, Case3)

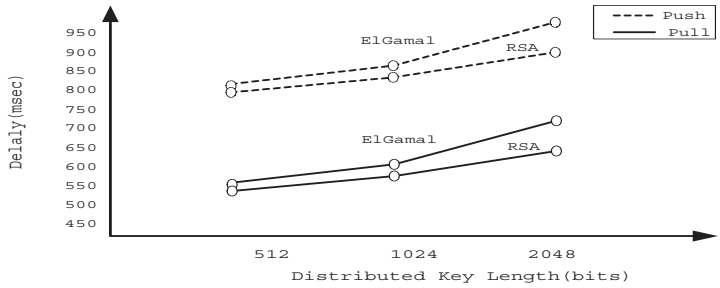

Fig. 4. Delay Comparison using Public key encryption algorithms(Case2, Case4)

4.2 Experiment Results

In figure 3, we analyzed delay time considering basic round trip time of proposed Push and Pull-typed model with symmetric key encryption algorithms and its distributed key length. In this performance simulation, we used DES-EDE and DES as a symmetric key algorithm. We can see that proposed push typed model has about 750msec of delay time and pull typed model has about 500msec of delay time(As illustrated Fig. 3.) In the figure 4, we analyzed the delay time considering the basic round trip time of proposed Push and Pull-typed model with the public key algorithms and its distributed key length. In this performance simulation, we used RSA and ElGamal as a public key algorithm. If the proposed models distribute the secret key more than 2048bits of key length, we see that, on average, the delay between ElGamal and RSA, is about 914msec for the push model and about 664msec pull model(As illustrated Fig. 4.).

In the result of performance analysis, we can know that Pull typed model using symmetric algorithm(Case 3) has the shortest delay among the proposed four cases. Also, though there was basically 250msec of delay time difference between proposed Push and Pull models, if key distribution method with Pull scheme employs public key algorithm which has more than the key size of 2048bits(Case 4) and if key distribution method with Push scheme employs symmetric encryption algorithm(Case 1), the difference of entire delay time between the models decreases to 87msec. Thus, the propagation delay of satellite networks is the biggest factor to affect communication delay between the terminals. In other words, when we consider the propagation delay of satellite environments, the encryption algorithm processing speed of various key distribution models doesn't influence the total delay of satellite communication much, so we need appropriate choice according to its application purposes.

5 Conclusion

In this paper, we have studied the security threats in satellite communication environments, their considerations and various key distribution models. After that, we proposed four kinds of key distribution models such as Push typed key distribution model using symmetric key encryption algorithm and public key encryption algorithm, Pull typed key distribution model using symmetric key algorithm and public key encryption algorithm as a method of information security in satellite networks, and made modeled of satellite communication system in accordance with its characteristic.

Through the performance analysis of proposed key distribution models using our simulation equations, we can see that, if the Pull typed key distribution model using public key algorithm distributes more than the key size of 2048bits, the difference of delay time between the four models is decreased below 87msec. Thus, through the performance analysis of the proposed four key distribution model, we can see the possibility of application of them to satellite networks, though they use different encryption algorithm and key distribution schemes.

Potential future work will include additional effectiveness testing with various key distribution models and encryption algorithms.

References

1. ANSI, *X9.17 Financial Institution Key Management Standard*, X9-Secretarait Banker Association, 1985
2. National Institute of Standards Technology, *Framework for National Information Infrastructure Services*, NISTR 5478 (Gaithersburg, MD: NIST, July 1994).
3. Bruce Schneier, *Applied Cryptography*, Wiley, pp53 64, 1996
4. Alfred J. Menezes, *Handbook of Cryptography*, pp497 514, CRC Press, 1997
5. S.W.Kim, *Frequency-Hopped Spread-Spectrum Random Access with Retransmission Cutoff and Code Rate Adjustment*, IEEE, Vol.10, No.2, Feb 1992
6. Hyoun K., *Traffic Control and Congestion Control in ATM over Satellite Networks*, IEEK, Vol.4, No.1, Nov 1998
7. Jerry Banks, *Discrete-Event System Simulation*, Prentice-Hall, pp264-265, 1996
8. Kyung Hyune Rhee, *Delay Analysis on Secure Data Communication*, KIISC, Vol.7, No.12, Dec 1997
9. William Stallings, *Cryptography and Network Security*, Prentice-Hall, pp 292-293

Appendix

Table 4. Symmetric Encryption Algorithm Processing Time

Algorithm	Bytes Processed	Time Taken	Mbps
DES	134217728	9.945	102.968
DES-EDE	33554432	6.740	37.984
RC5	536870912	12.988	315.368
Blowfish	134217728	7.091	144.408
MD5-MAC	1073741824	12.078	678.256

Table 5. Public key Encryption Algorithm Processing Time(msec/operation)

Algorithm	Encryption	Decryption	Signature	Verification
RSA 512	0.14	1.93	1.92	0.13
RSA 1024	0.32	10.23	10.29	0.30
RSA 2048	0.89	64.13	64.13	0.85
ElGamal 512	2.62	1.37	-	-
ElGamal 1024	11.03	5.77	-	-
ElGamal 2048	49.19	25.35	-	-