A Lightweight and Secure Routing Strategy in Satellite Networks

Ruiyan Cai [1, 2, a], Delin Liao [1, 2, b], Li Yang [1, 2, c], Chengsheng Pan [2, d]

[1]College of Information Engineering, Dalian University, Dalian 116622, China;

[2] Communication and Networks key Laboratory, Dalian 116622, China;

[a]34010361@qq.com, [b]liao1137@126.com, [c]yangli945@126.com, [d]pancs@sohu.com

Abstract

Nowadays, the problem of information security is so serious, In view of the lack of research on routing security in satellite networks, the satellite environment and the limited capacity of satellite storage and computing. Based on the certificateless cryptosystem, this paper proposes a lightweight certificateless signcryption routing strategy, which solves the problem of fusion between the signcryption algorithm and the routing algorithm. While ensuring the security of routing, it improves the encryption The efficiency, saving computing and storage resources, At the same time, a scheme to prevent internal attacks is given, which makes the function of the secure routing strategy more perfect. Simulation shows that this strategy has a strong defense capability and can provide security for satellite networks.

Keywords

Satellite network; Security routing; certificateless signcryption.

1. Introduction

With the accelerating exploration of space and the use of space resources, as well as the rapid development of Internet technology in recent years, the distance between people and satellites has been greatly shortened. As the popularity of satellite applications, hackers gradually reach out to the satellites. In recent years, frequent hacking of NASA spaceflight in many countries, theft of spacecraft data and satellite communications data, and the satellite has increasingly become the target of hacking attacks [1]. The security of satellite networks is becoming more and more prominent. However, the routing security of satellite nodes is more important in the entire satellite network security system. As with terrestrial networks, the security goal of satellite routing still needs to meet the requirements of data confidentiality, integrity, authentication, non-repudiation, etc[2] ,However, since the environment in which a satellite network is located and the resources it possesses are very different from the terrestrial network, it can not copy the security plan of the terrestrial network. The International Space Advisory Council (CCSDS [3]) introduced the SCPS family of communications protocols for satellite networks. The security protocol SCPS-SP [4] refers to an end-to-end information protection protocol proposed by IPSec in terrestrial network [5], which can guarantee the integrity, authentication, confidentiality, However, since this protocol does not have a user authentication mechanism, it can not defend against replay attacks initiated by relay nodes, and the security level defined in this protocol has not been actually applied [6].

Li Zhe et al proposed to add a trust mechanism in the satellite network routing [7], through the node trust to determine whether the node is attacked, and quickly respond to protect the entire network security, but the method is passive defense, only in The node will not react until it has been attacked. Peng Changyan and others used a broadcast-based signcryption scheme [8] to propose an on-demand routing protocol that is suitable for LEO satellite network security. This scheme has a strong defense against external attacks, but it lacks internal attacks consideration. Hao Xuanwen proposed an

authentication routing protocol based on double-layer satellite networks [9], and proved the security performance of the protocol. However, since the certificate authentication method is still adopted, it not only increases the authentication time but also increases the storage and computing capabilities demand. Overall, the current research on satellite network security routing is scarce, most of them refer to terrestrial Ad hoc networks, and lack of global considerations, there is still no uniform standard for routing security goals.

Considering the characteristics of satellite networks, this paper proposes a lightweight satellite network security routing strategy that hopping hop-by-hop encryption and verifying routing control information based on the characteristics of satellite networks. It can not only ensure the security of routing nodes, but also shorten the node authentication times and time, but also have the ability to defend against internal attacks, which can effectively resist hacker attacks and enhance the survivability of satellite networks.

2. Certificateless signcryption system

In 2003, Al-Riyami and Paterson proposed a certificateless public key system [10]. In this system, the user's private key is no longer completely managed by a trusted third party, but is divided into two parts, one part is generated by the key generation center (KGC) and the other part is generated by the user himself, this can be a good solution to the key escrow problem.

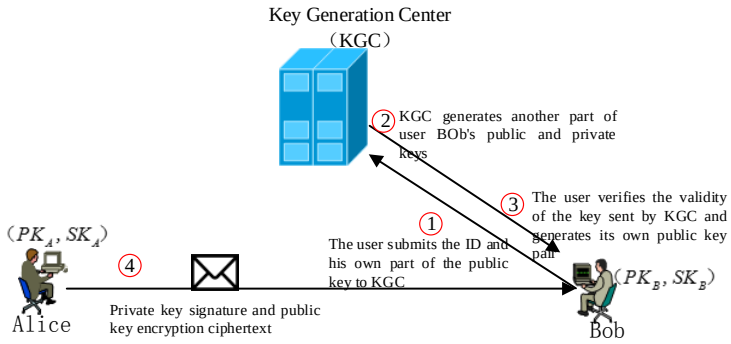

Fig. 1 Certificateless cryptosystem infrastructure

Barbosa and Farshim first presented a certificateless signcryption scheme in 2008 [11], which uses the method of bilinear pair mapping to apply certificateless signcryption, but, this scheme is a large amount of calculation, computational efficiency is low.

After 2010, researchers have successively proposed a certificateless signcryption scheme without bilinear pairings. However, although its computational efficiency has been improved in [12], its security still has some defects of different levels, literature [13] pointed out that a more efficient program is proposed, but its security is obviously inadequate. After considering the security and computational complexity, the paper [15] gives a highly efficient certificateless signcryption scheme and proves that this scheme has better computational efficiency and security in the existing signcryption scheme. Literature [16] further optimizes the steps and complexity of the algorithm, which not only makes the execution process more concise but also has higher safety performance. The program is vividly described in Fig. 1, and the detailed implementation process is as follows.

2.1 establish system parameters

KGC selected three anti-collision hash function, and randomly select the master key s to save the system to calculate the public key P_{Pub}, And open the system parameter params to the user.

2.2 User's key generation

The user i chooses the master key x_i randomly, calculates its own part of the public key X_i and sends it to KGC, KGC generates another part of the public key Y_i and the private key y_i, and passes the

secret channel to the user i, finally, the complete public key pair (PK_i, SK_i) of the user is generated, in which the public key $PK_i = (X_i, Y_i)$ and the private key $SK_i = (x_i, y_i)$.

2.3 signcryption process

If Alice wants to send Bob a message, Alice will use her own private key SK_{Alice} and Bob's public key PK_{Bob} to encrypt the plaintext message and send the signed message to Bob.

2.4 Decryption process

After Bob receives the signed information sent by Alice, Bob decrypts it with his private key SK_{Bob} and Alice's public key PK_{Alice}, verifies the validity of the signature and identity, and if so, accepts the decrypted information. Otherwise, The information is not reliable, discard the packet, decryption failed.

Compared with traditional PKI system based on PKI, Certificateless public key cryptography is similar to Identity-based cryptography, they bind the user's public key to the user's identity, do not need to use the certificate back and forth multiple times to verify user identity. At the same time, the certificateless password system eliminates the problem that the entire private key of all the users in the identity-based cryptosystem is entrusted by trusted third parties to trigger the key leakage. Therefore, certificateless public key cryptosystem not only combines the advantages of two Cryptosystems Based on PKI and ID, but also overcomes their shortcomings to a certain extent. It is an excellent public key cryptosystem which is very suitable for satellite network applications.

3. Design of Lightweight Space Network Security Routing Strategy

3.1 Satellite network model

In this paper, a number of high-rise orbit satellite network as a key generation center (KGC), for all LEO satellite nodes to provide key distribution services. As shown in Fig. 2, in a satellite network, the coordinates of each satellite can be expressed as (N_i, M_i), N_i represents the orbital plane where satellite i is located, M_i represents the position of satellite i in orbit. If $Sate_i$ is used to represent the identification information of satellite i, the unique identifier of each satellite can be expressed as $ID_i = Sate_i \| (N_i, M_i)$.

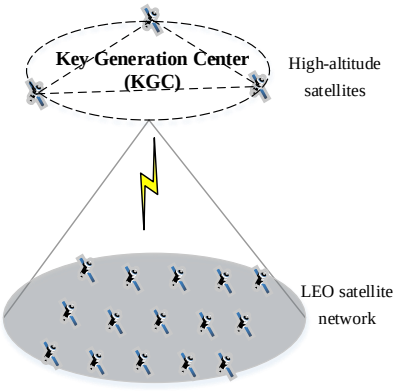

Fig. 2 Satellite network model

3.2 Security Routing Protocol

Based on certificateless signcryption, this paper designs a Certificateless Signcryption Secure Routing (CSR) protocol for signcryption of routing control information in satellite networks. The protocol is divided into routing initialization, routing discovery, and routing maintenance three parts.

3.2.1 Routing Initialization

This phase mainly completes the system parameters generation and protocol initialization. First of all, KGC chooses an order G as a cyclic group G, P is a generator of G, and selects three anti-collision hash functions, $H_1:\{0,1\}^{l_1}\times G\times G\to Z_q^*$, $H_2:\{0,1\}^{l_1}\times\{0,1\}^{l_2}\times G\times G\to Z_q^*$, $H_3:\{0,1\}^{l_1}\times G\to\{0,1\}^{l_2}$ (where Z_q^* is a finite multiplicative group of degree q, l1 is the bit length of the user ID, and l2 is the bit length of plaintext information). Then KGC randomly selects the system master key $s\in Z_q^*$, calculates the system public key $P_{Pub}=sP$, and discloses the system parameters $Params=\{q,G,P,P_{Pub},H_1,H_2,H_3\}$. User i randomly chooses the secret value $x_i\in Z_q^*$, calculates part of the public key $X_i=x_ip$, and sends IDi and X_i to KGC. Then KGC randomly chooses $r_i\in Z_q^*$, calculates another part of user i's public key $Y_i=r_iP$ and partial private key $y_i=r_i+sH_1(ID_i,X_i,Y_i)$, and returns them to user i through the secure channel. Finally, the user starts to calculate his private key pair (PK_i,SK_i) after receiving it, where the public key $PK_i=(X_i,Y_i)$ and the private key $SK_i=(x_i,y_i)$. Node i verifies whether part of the private key issued by KGC is valid by the following formula.

$$y_iP=Y_i+P_{Pub}H_1(ID_i,X_i,Y_i) \tag{1}$$

3.2.2 Routing Discovery

When a node in the network wants to communicate with another node but neither reaches the routing table of the other, it needs route discovery to find a path to the best path to the destination node and add it to the routing table . Routing discovery includes routing request and routing reply in two parts.

a) routing request

Assume that the path of routing discovery as shown in Fig. 3.

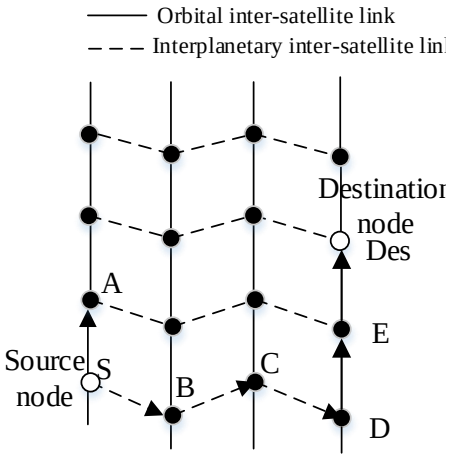

Fig. 3 Routing discovery

If the source node S wants to send information to the destination node Des but does not have the corresponding routing information, the source node firstly uses its own private key $SK_S=(x_S,y_S)$ and the public key $PK_{Des}=(X_{Des},Y_{Des})$ of the destination node to do certificateless signcryption on the routing request information. Detailed signcryption process is as follows:

Source node S randomly selects $u\in Z_q^*$, calculates $Q=uP$, and then calculates $W=u(X_{Des}+Y_{Des}+P_{Pub}h_{Des})$, where $h_{Des}=H_1(ID_{Des}+X_{Des}+Y_{Des})$, and generates a ciphertext:

$$C=m\oplus H_3(ID_{Des},W) \tag{2}$$

Then calculate the signature value:

$$V=n(x_S,y_S)+u_k \tag{3}$$

among them $n=H_2(ID_S,C,X_S,Q)$, $k=H_2(ID_S,C,Y_S,Q)$.

Finally, we get the signed information $\sigma=(Q,V,C)$, we use $SG_{S,Des}(RREQ)$ to represent the whole process. Meanwhile, in order to verify the identity of the sending node and the integrity of the information sent, the sent plaintext (RREQ) needs to be signed by using the private key of the sending

node (S), and the signature value is denoted by $S_S(RREQ)$. Finally, the source node obtains the desired broadcast Information:

$$< RREQ \| S_S(RREQ) \| SG_{S,Des}(RREQ) > \quad (4)$$

The first part of this broadcast message is plaintext RREQ, the reason is that the routing request is broadcast on the way. The plaintext approach not only reduces the amount of computation but also does not require worrying even if the information is tampered with because the latter two pieces of information are noticeable. The second part $S_S(RREQ)$ is the signature of the sending node on the message sent so that not only the identity of the sending node can be verified, but also the integrity of the RREQ. The third part is only the purpose of the node Des to unlock, its purpose is to prevent malicious tampering with the intermediate node routing request information, the purpose of the node after the first part of the information will be compared with the unmatched, then the packet is invalid will be discarded.

After the intermediate node X receives the broadcast message, it verifies the sequence number in the RREQ and the signature value of the previous hop to determine the source of the information. If authentication passes, the TTL in the RREQ is decremented by 1 and the new RREQ message is signed with its own private key, plus a packet that can not be decrypted to get the packet that node X broadcasts to the neighbor:

$$< RREQ \| S_X(RREQ) \| SG_{S,Des}(RREQ) > \quad (5)$$

Other nodes repeat similar actions until the destination node Des receives the routing request message. The destination node verifies the sequence number of the RREQ and the signature value of the previous hop for the first RREQ signcryption information, and starts the de-signcryption if all passed. The detailed process is as follows.

First verify the signature value:

$$VP = n(X_S + Y_S + P_{Pub}h_S) + kQ \quad (6)$$

Among them $h_S = H_1(ID_S + X_S + Y_S)$, the plaintext is calculated if the verification is successful:

$$m = C \oplus H_3(ID_{Des}, W') \quad (7)$$

where $W' = (x_{Des} + y_{Des})Q$, If the signature verification does not pass, then no need to continue to decrypt the plaintext, directly discard the packet, the routing discovery process is completed, as shown in Fig 4.

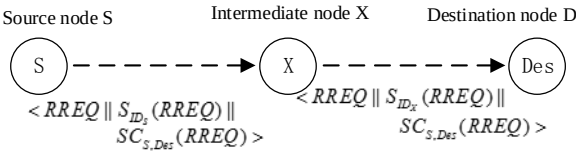

Fig. 4 Routing discovery process

2) routing reply

The destination node responds to the first arrived routing request message and sends the signaled routing reply message hop by hop along the opposite path of the routing request.

Taking the path in FIG. 3 as an example, the destination node Des signs the routing reply (RREP) information using its own private key and the public key of the next hop node (E) to obtain the $SC_{\mathrm{Des},E}(RREP)$. At the same time, in order to enhance the capability of defending against internal node attacks, the RREP information needs to be signcrypted using the private key of the destination node and the public key of the source node to obtain the $SC_{\mathrm{Des,S}}(RREP)$ (this part of information intermediate node can not decrypt the secret until it reaches the source node S). Finally, get the routing response information to be sent:

$$< SC_{\mathrm{Des},E}(RREP) \| SC_{\mathrm{Des,S}}(RREP) > \quad (8)$$

Node E sends it to the next hop node D. Node D receives the message and uses S and Q to decrypt the previous part according to the formula. If the de-signing is successful, RREP information will be obtained; the routing table will be updated and the RREP information will be re-signed. The

information for de-signing will be sent to the next hop node. The intermediate node X above operation is repeated until the packet reaches the source node S.

When the source node S receives the $< SC_{B,S}(RREP) \| SC_{Des,S}(RREP) >$ packet sent by the node B on the previous hop, the source node S separately decrypts the two pieces of information in the packet. If both the legitimacy of the signature and the integrity of the data are passed, two RREP messages are obtained, and the information such as the source address and the destination address is compared with each other. If they are the same, it indicates that there is no malicious tampering with the intermediate node, the information is credible, and update the routing table according to the information in the RREP, as shown in Fig. 5.

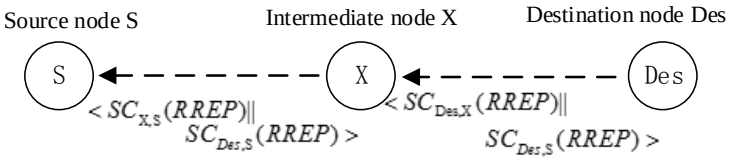

Fig. 5 routing reply packet change process

3.2.3 Routing maintenance

Due to the dynamic nature of the satellite link and node congestion, some nodes on a link may be temporarily blocked. In order to maintain the validity and confidentiality of the path, we periodically broadcast the HELLO packet to detect the status of the neighbors on the link . When it is found that the neighbor node is faulty, the node sends encrypted RERR (route error) information to the neighboring nodes on the link. After the node receives the encrypted information, it verifies the validity of the information, and then acts accordingly according to the information in the RERR, and signs the RERR information to the next neighbor node in the link until all nodes on this link have received this signed message.

The following still takes the link {S B C D E Des} in FIG. 2 as an example. If node D fails and is unreachable, both nodes C and E can detect that nodes C and E will sign the RERR information and send it to neighboring nodes on the link. Take node C as an example, node C uses its own private key and B's public key to sign RERR information:

$$< SC_{C,B}(RERR) > \tag{9}$$

And send it to Node B. When the node B receives the message, it decrypts it by using its own private key S_B and C's public key Q_C and verifies the integrity of the message and the validity of the signature. If the authentication is passed, update its own routing table, and use its own private key and node S's public key to sign RERR information and send it to node S, as shown in Fig. 6:

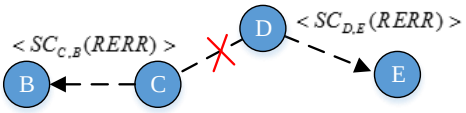

Fig. 6 Routing maintenance process

3.3 Internal attack defense

Although we defend most of the external intrusion through the above method, but still lack of consideration of attacks from within the network, Fig. 7 is a model diagram of the internal network attacks.

When an ordinary node is invaded and captured, it becomes an antecedent of possible internal attacks. Internal attacks are divided into passive attacks and passive attacks. These attacks not only steal data from the network, but also destroy other normal nodes, which will seriously cause the entire network service to collapse.

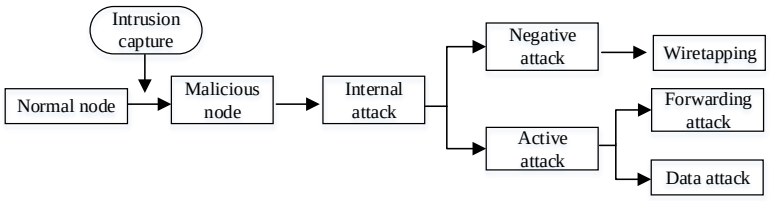

Fig. 7 Internal Attack Model

So, we designed a program called Monitor to monitor the behavior of each node's routes. Monitor requires that each routing node must run it. The working principle is that the sender of the data packet still needs to monitor the processing behavior of the next hop node route through the Monitor program after the data packet is handed over to the next hop. If the next hop is not the destination node of the data packet and the next hop node does not correctly forward the data packet, it considers that the next hop node has a problem. Of course, if a node frequently sends routing requests to the network, the route discovery is seldom successful, and the node also determines that there is malicious behavior. Of course, if a node frequently sends routing requests to the network, the route discovery is seldom successful, and the node also determines that there is malicious behavior, and notify other nodes to avoid these problem nodes when routing, thus isolating malicious nodes. The working process shown in Fig. 8.

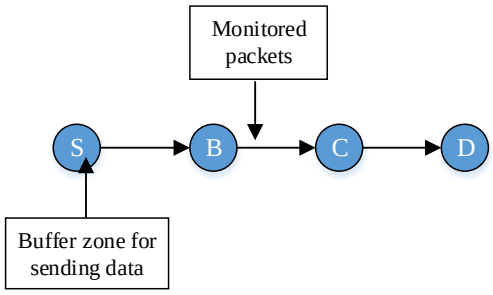

Fig. 8 Monitor the working process

By maintaining the most recently-sent packet buffers for routes, we compare each packet being snooped with the one in the buffer and, if matched, indicate that the packet has been correctly forwarded. The packet in the buffer will be deleted by the watchdog and forgotten. If a packet stays in the route buffer for more than a certain amount of time, the watchdog keeps track of the number of failed packets. If this number exceeds a certain threshold, it is determined that there is an abnormal behavior on the node and the other nodes are informed that the malicious node is quickly isolated from each other to implement active defense.

4. Safety analysis

The certificateless signcryption scheme is based on the identity-based signcryption to optimize the trusted third party, solves the key escrow problem, and prevents the private key generation center from disclosing the private key of the user. This not only defends against man-in-the-middle attacks, but also achieves true key uniqueness.

When a new route is added to the network, it gets a pair of public-private key pairs. Because the public and private keys are unique, the public key binds the user's identity to its ID, while the private key only has it. This allows it to meet the confidentiality and non-repudiation, and signing process makes it to ensure data integrity and authentication, so the scheme can achieve the routing protocol security goals.

We protect nodes against attacks by routing messages without certificates, and in the meantime, we take defense of internal attacks into account. Through the Monitor program to monitor each node in the last hop to receive information sent after the action made to determine whether the forwarding node malicious behavior. If a malicious node is found, Monitor will notify the other node and isolate the malicious node. Through these two methods makes the routing security strategy more secure and more complete.

5. Simulation analysis

At present, the research of satellite network security routing is scarce, mostly referring to terrestrial Ad hoc networks. In order to verify the validity of the security routing strategy proposed in this paper, we compare the performance of the Ad-hoc On-Demand Distance Vector routing protocol (AODV) [17] with the more secure CSRP [18] Routing protocol, as well as the Certificateless Signcryption Secure Routing (CSR) proposed in this paper. This article evaluates routing performance from the following two aspects:

(1) Average time for establishing a route: The average time spent by the source node from sending routing request information to receiving routing response information, which is used to evaluate the time cost of the routing protocol.

(2) Routing Costs in Forged Packet Environment: The routing overhead of different algorithms under different fake packet proportions can be used to evaluate the validity of routing policies.

5.1 simulation environment

We use opnet14.5 to simulate the Iridium satellite polar orbit constellation; the specific parameters are shown in Table 1.

Table 1 Iridium satellite constellation parameters

Parameter type	Parameter configuration
Orbit height	780km
Number of tracks	6
Orbital plane number of satellites	11
Orbital inclination	86.4°
Orbital plane interval	31.6°
Interstellar link latitude threshold	60°
The number of each satellite inter-satellite link	4
Satellite link error rate	10^{-5}
Interplanetary link bandwidth	10Mb/s
Uplink / downlink bandwidth	1.5 Mb/s

5.2 Simulation Results Analysis

Fig. 9 shows the average establishment time comparison of different routing strategies. As can be seen from the figure, the average routing establishment time value is ADOV, CSR and CSRP. Because ADOV is a routing that does not use an encryption algorithm, it takes the shortest amount of time. The CSR (Certificateless Signcryption Secure Routing Policy) uses 15-20% more time than ADOV in this article because it takes extra time for routing control signaling signing and signing, while CSRP takes the most time, 28% more than ADOV, 10% more than CSR. CSRP is relatively complex and redundant in terms of architecture and algorithm with respect to CSR. Each data packet sent by such a route needs to be forwarded by a trusted intermediate node, which severely reduces the data packet forwarding rate , and extended routing establishment time.

Fig. 10 shows the routing costs of different routing policies in different proportions of routing forged packets. As can be seen from the figure, when there is no route fake packet in the network, the routing cost of the security algorithm is slightly larger than that of the ordinary algorithm. However, when a large number of routes are forged in the network, ordinary routing algorithms do not recognize the packets, and the forged packets are still forwarded. As a result, the routing overhead gradually increases. However, the secure routing algorithm in this paper has a strong defense capability against

routing forged packets because it is hop-by-hop to verify the security of routing control packets. When it is detected that the data packet is forged, it will be discarded when it is invalid and will not be forwarded any longer. So, the routing cost will not increase too much. Among them, the routing overhead based on certificateless signcryption and identity-based signcryption is similar, but it is obviously superior to CSRP algorithm.

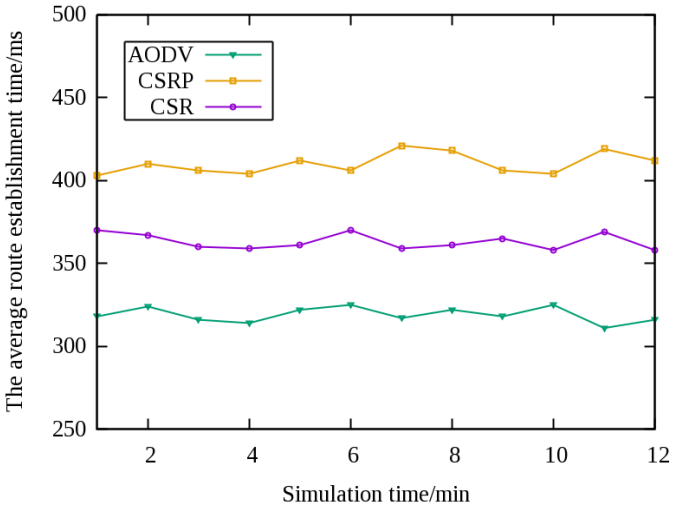

Fig. 9 The average routing establishment time

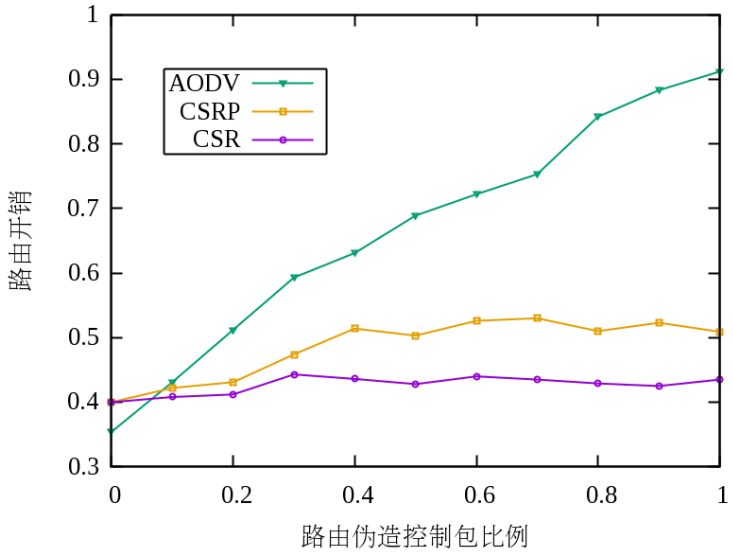

Fig. 10 Routing Costs in Forged Packet Environment

6. Conclusion

Based on the certificateless cryptosystem, this paper proposes a lightweight routing strategy for certificateless signcryption in space networks. In this secure routing strategy, the third party used to authenticate the user no longer hosts the complete private key of all users, which effectively solves the problem of key leakage. At the same time, we solve many problems that signcryption algorithms encounter in routing and design a method to defend against internal attacks, which makes the defense ability of routing more complete and greatly enhances the survivability of space network.

Acknowledgements

This subject is supported by National Natural ScienceFoundation of China (NSFC Grant No. 61722105).

References

[1] Wei Yang - Satellite - the next hacker attack "front" vigilance! Hacker's "claws" has been extended to the "sky"! [J]. Information Security and Communications Security, 2016 (1): 62-63.

[2] ZHOU Xing, LIU Jun, DONG Chun-hong, et al. Research on satellite network security routing goal [J] .Computer Technology and Development, 2013, 23 (7): 163-166.

[3] Delivery C F, Book B. Consultative Committee for Space Data Systems. Panel 1: Support[J]. Journal of Spacecraft Tt & C Technology, 1987, 85.

[4] CCSDS 713.5-B-1 SPACE COMMUNICATIONS PROTOCOL SPECIFICATION (SCPS) — SECURITY PROTOCOL (SCPS-SP) [S].1999.

[5] Kent S, Atkinson R. Security Architecture for the Internet Protocol[M]. RFC Editor, 1998.

[6] LIAO Yong, CHEN Hong-yu, SHEN Xuan-fan.An Improved SCPS-SP in Spatial Information Networks [J] .Computer Science, 2017, 44 (6): 155-160.

[7] Li Zhe, Liu Jun, LIZhe, et al.Study on satellite network security routing [J] .Journal of Communications, 2006,27 (8): 113-118.

[8] Peng Changyan, Zhang Quan, Tang Chaojing.A secure on-demand routing protocol in LEO satellite network [J]. Signal Processing, 2010, 26 (3): 337-346.

[9] Hao Xuanwen, Ma Jianfeng, Ren Fang, Liu Xiaoyue, Zhong Yantao.A certified routing protocol based on double-layer satellite network in spatial information network [J] .Computer Science, 2011,38 (02): 79-81.

[10] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography[M]// Advances in Cryptology - ASIACRYPT 2003. Springer Berlin Heidelberg, 2003:452-473.

[11] Barbosa M,Farshim P Barbosa M, Farshim P. Certificateless signcryption[C]// ACM Symposium on Information, Computer and Communications Security. ACM, 2008:369-372.

[12] ZHU Hui, LI Hui, WANG Yu-min. Certificateless signcryption scheme without bilinear mapping. Computer Research and Simulation. 2010

[13] He Debiao. Security analysis of certificateless signcryption mechanism. Journal of software. 2013

[14] Liu Wenhao, Xu Chun Xiang. Non-bilinear matchless certificateless signcryption scheme. Journal of software.2010

[15] ZHOU Yan-wei, YANG Bo, ZHANG Wen-zheng. Security analysis and improvement of certificateless signcryption scheme without bilinear mapping [J] . Chinese Journal of Computers, 2016, 39 (6): 1257-1266.

[16] ZHOU Yan-wei, YANG Bo, WANG Qing-long. Security analysis and improvement of certificateless signcryption scheme without bilinear pairing. Journal of Software.2017

[17] Perkins, BeldingRoyer. Ad hoc On-Demand Distance Vector (AODV) Routing[J]. Rfc, 2003, 6(7):90.

[18] Bhoi S K, Faruk I H, Khilar P M. CSRP: A Centralized Secure Routing Protocol for mobile ad hoc network[C]// Third International Conference on Emerging Applications of Information Technology. IEEE, 2013:429-432.