ML-IKE: A Multilayer IKE Protocol for TCP Performance Enhancement in Wireless Networks*

ZHANG Ya-Hang[1,2+], CHENG Bo-Wen[1,2*], QING Si-Han[2], ZOU Guang-Nan[1], WEN Wei-Ping[2]
1(Space Star Technology Co.,Ltd, Beijing 100081, China)
2(Department of Information Security, SSM, Peking University, Beijing 100084, China)
+ Corresponding author: Phn: +13488694401, E-mail: zhangyahang@gmail.com
* Corresponding author: Phn: +13488694376, E-mail: shuanshui_66@163.com

ABSTRACT

To solve the conflict between TCP accelerating technology based on PEP middle node and IPSec protocol used in the Satellite Network, NASA and the Hughes Research Laboratory (HRL) each independently proposed a solution named Multilayer IPsec protocol which can integrate IPSec with TCP PEPs. The problem is: Traditional IKE protocol can't work with Multilayer IPSec protocol. In this study, the traditional IKE main mode and quick mode are enhanced for layered IPSec protocol, and an improved layered key distribution protocol: ML-IKE is proposed. This key distribution protocol is used for key exchange between peers and middle node, so that different nodes have different security associations (SA), and different security associations correspond to different IP packet fields, so different SA nodes have different authorization to different IP packet fields. ML-IKE protocol is suitable for layered IPSec, thus layered IPSec can be used for automatic key distribution and update.

1. INTRODUCTION

Satellite network has advantages of high speed, wide transmission range and so on. As the space technology developing, Satellite systems are rapidly changing their role from the "bent-pipe" transparent channel paradigm to the on-board routing regenerative paradigm [1]. But TCP which is the primary transport protocol is no longer suitable in satellite networking environment, due to long propagation delay and significant packet losses on the satellite link in land mobile satellite channels [2][3]. To eliminate this conflict, many new TCP proposals such as the TCP Hybla [4], Split TCP [5], TCP Westwood [6] and TCP-Peach [7] used in TCP PEP mechanisms are presented and discussed.

These nonstandard TCP protocols bring new design problems at network layer, since when an end-to-end security mechanism, such as IPsec, is used, TCP PEP mechanisms can not work. This is because that IPsec encrypts and/or authenticates the fields that the TCP PEP needs read/write access [8]. To solve this problem, NASA [9] and the Hughes Research Laboratory (HRL) [10][11] each independently proposed a solution named Multilayer IPsec protocol which can integrate IPsec with TCP PEPs, Researchers in Amirkabir University of Technology and Harbin Institute of Technology improved it and developed ML-IPsec+[12] and CZML-IPsec[13]. It allows wireless network operators or service providers to grant base stations or wireless routers limited and controllable access to the TCP headers for performance enhancement purposes. But traditional IKE protocol is only able to establish security associations and obtain authenticated keying materials between two IPsec endpoints (hosts or security gateways), which means that the traditional IKE protocol is not suitable for multilayer IPsec protocol.

In this paper, the traditional IKE is improved, and an improved layered key exchange protocol: ML-IKE (Multilayer Internet Key Exchange) is developed. The rest of this paper is organized as follows: In Section 2, the notion of ML-IPsec is explained. Section 3 described the notion of traditional Internet Key Exchange Protocol. Our approach is presented in Section 4. Section 5 states the conclusion and future work.

2. ML-IPSEC

The PEP nodes based on TCP acceleration technology in satellite links need to read and write TCP Header in IP packets. It is a conflict to traditional IPsec and breaks the end-to-end protection model of IPsec. ML-IPsec is the solution developed to solve this problem. The main idea of this protocol is to divide the IP datagram into several parts and apply different forms of protection to different parts. For example, in the satellite network based on TCP acceleration

International Conference on Space Information Technology 2009, edited by Xingrui Ma, Baohua Yang, Ming Li,
Proc. of SPIE Vol. 7651, 765102 · © 2010 SPIE · CCC code: 0277-786X/10/$18 · doi: 10.1117/12.855391

technology, the TCP payload part can be protected between two end points using SA1 while the TCP/IP header part can be protected and accessible to two end points plus certain routers in the network using S2 (As shown in Figure 1). It allows TCP PEP to coexist with IPsec, and provides both performance improvement and security protection to wireless networks [10].

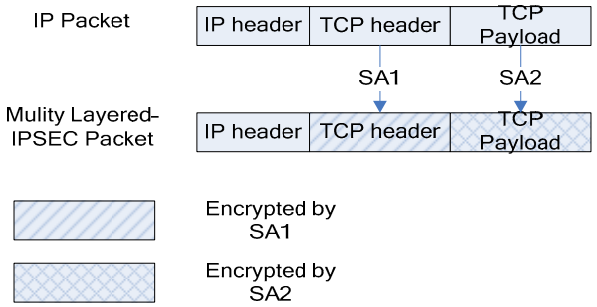

Figure 1 Packet Encryption in ML-IPsec

3. TRADITIONAL INTERNET KEY EXCHANGE PROTOCOL

Internet Key Exchange (IKE) is a hybrid of the ISAKMP framework and the Oakley and SKEME protocols. It negotiates the IPsec security associations (SAs). This process requires that the IPsec systems first authenticate themselves to each other and establish shared keys. Oakley and SKEME each define a method to establish an authenticated key exchange. These include payloads construction, the information payloads carry, and the order in which they are processed and how they are used. While Oakley defines "modes", ISAKMP defines "phases" [14].

Traditional IKE needs two phases to establish IPsec SA. In phase 1, IKE creates an authenticated, secure channel between the two IKE peers, called the IKE security association. "Main Mode" and "Aggressive Mode" each accomplish a phase 1 exchange. Figure 2 described the "Main Mode" with a pre-shared key in the first phase of IKE.

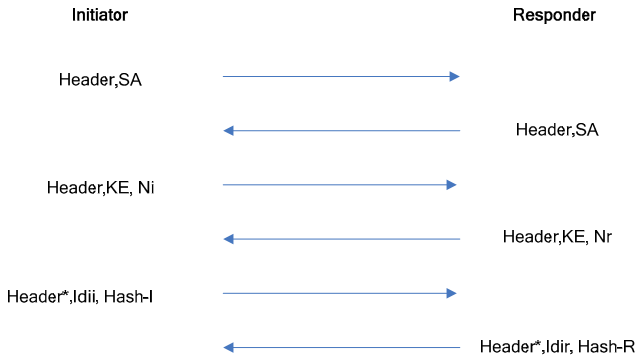

Figure 2 Main mode with a pre-shared key

In Phase 2 the Security Associations are negotiated on behalf of services such as IPsec or any other service which needs key material and/or parameter negotiation. "Quick Mode" accomplishes a phase 2 exchange. Figure 3 described the "Quick Mode" with a pre-shared key in the second phase of IKE.

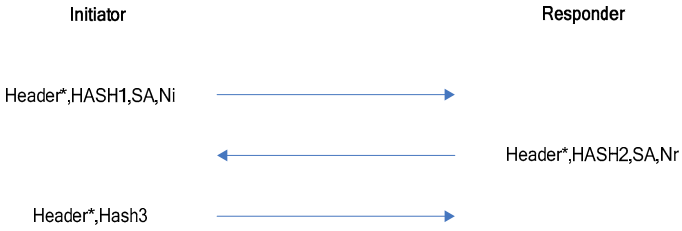

Figure 3 Quick mode with a pre-shared key
Multilayer Internet Key Exchange Protocol

As described in section 1, traditional IKE is not suitable for Multilayer IPsec Protocol, And ML-IKE solution was developed for ML-IPsec used in the satellite network based on traditional IKE.

In our solution, initiator node starts the ML-IKE Exchanges, and the middle nodes will also take part in the ML-IKE process. And when the exchanges complete, the Initiator and the Responder will share IPsec SA2 while the Initiator, Responder and the trusted PEP intermediate node will share IPsec SA1. Then the TCP header will be protected by IPsec SA1 while the TCP payload protected by IPsec SA2. The network topology Diagram is shown in Figure 4. Like the traditional IKE, the basic operation of ML-IKE can be broken down into two phases. Until now, we just extend the main model in the first phase and quick model in the second phase using pre-shared keys encryption to authenticate the exchange.

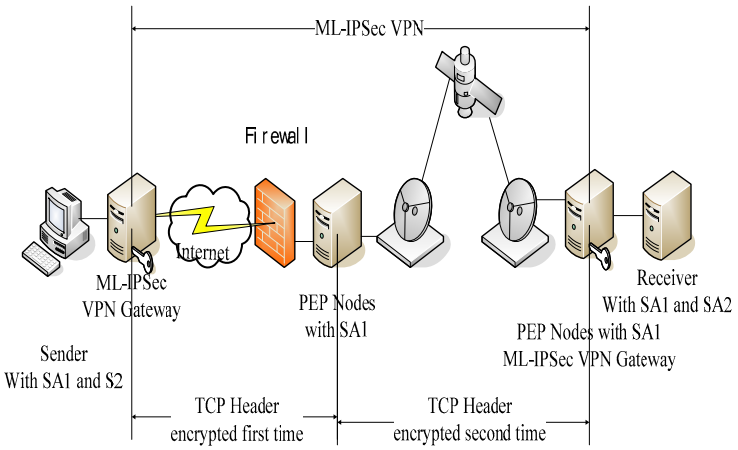

Figure 4 Satellite network Accelerated VPN Network Diagram

3.1 Phase 1: The Main Model of ML-IKE

The main model of ML-IKE in the first phase, which is the extension of main mode of traditional IKE, has 17 messages compared to 6 messages in traditional main model. The first 11 messages are used to exchange the parameters and key materials required to establish the IKE SAs while the last 6 messages are used to make authentications among IPsec endpoints and PEP node.

When using pre-shared key encryption for authentication, Main Mode in phrase 1 of ML-IKE is defined as shown in Figure 5. Main Mode accomplishes security association negotiation. And Security Association options takes the form of Transform Payload(s) encapsulated in Proposal Payload(s) including Security Association (SA) payload(s). If multiple options are made for phase 1 exchanges (Main Mode and Aggressive Mode) they must take the form of multiple Transform Payloads for a single Proposal Payload in a single SA payload. From another point of view, there must not be multiple Proposal Payloads for a single SA payload and there MUST NOT be multiple SA payloads in phase 1 exchanges. The goal of phase 1 is to form IKE-SA1 to protect all three participants' exchanges and IKE-SA2 to protect two endpoints' exchanges in phase 2. In this diagram, all these 17 messages can be divided into three function groups. Messages 1-5 belong to the first group, and they are used to negotiate policy, exchange Diffie-Hellman public values and ancillary data which are necessary for the exchange and identities. The content of message 1 is the same with of message 2. In the main model of phase 1, the Initiator node sends the message 1 and message 2 to start the negotiation. For phase 1, exchanges can only contain one SA payload, and one single SA payload includes only one Proposal Payload.

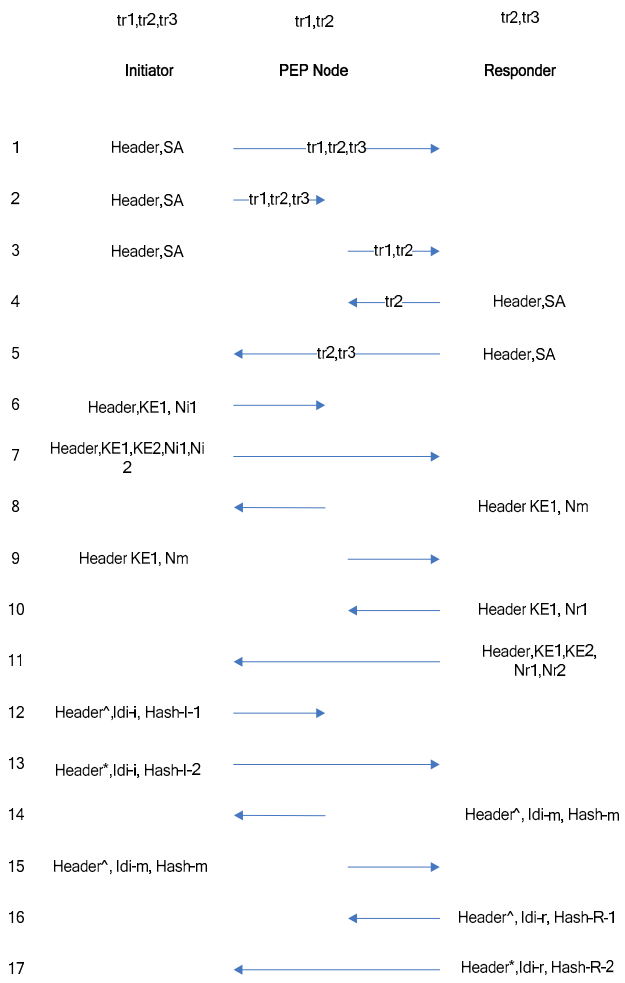

Figure 5 Exchanges of Main Model in ML-IKE using pre-shared Key authenticate

There can be multiple Transform Payloads (contains the encryption algorithm and the Hash algorithm) encapsulated in this Proposal Payload. The PEP immediate node receives message 2, then chooses all the transform supported by itself and the Initiator, then sends message 3 which contains the transform intersection supported by the Initiator and PEP node to the Responder. When message 1 arrives, the Responder will select one transform from the transforms encapsulated in the Proposal Payload in message 1 as algorithms used by the two endpoints to form IKE-SA2. Analogously, the Responder will select one transform from the transforms interaction in message 3 as algorithms used by all of the three participators. After that, the Responder will choose transform A from message 3 for IKE-SA 1 and send transform A to PEP immediate node through message 4. Also, the Responder will choose transform B from message 1 for IKE-SA 2, then it to the Initiator through message 5. In the example described in figure.5, the Initiator supported three transforms (tr1, tr2 and tr3); intermediate nodes support two transforms (tr1 and tr2); the Responder support tr2 and tr3. After the first five exchanges among three nodes, the negotiation selected tr2 for IKE-SA2 and tr2, tr3 for IKE-SA1.

Messages 6-11 belong to the second function group, and are used to finish Diffie-Hellman exchanges. The Initiator node offers two nonce values: Ni1 and Ni2, the intermediate node offers one nonce value Nm, and the Responder node offers Nr1 and Nr2 as the initiator. Message 7 and message 11 contains two key exchange payloads which contain the public information exchanged in two Diffie-Hellman exchanges. The three DH public values in KE1 are used to calculate the three-nodes shared KEY1 through a modified DH algorithm [14][15] while the two DH public values in KE2 are used to calculate the two-endpoints shared KEY2 through DH algorithm.

Messages 12-17 belong to the third group, these messages are used to authenticate the participators and provide a proof of participation in the exchanges. All these six messages are encrypted using KEY1 and KEY2 formed after messages 6-11. In messages 12, 14, 15 and 16, the Header^ means the messages are protected by KE1 while in messages 13 and 17 the Header* means the messages are protected by KE2.

After the exchanges in phase 1 of ML-IKE, the negotiation of IKE-SA1 and IKE-SA2 is completed. The Initiator and Responder obtain the IKE-SA1 and IKE-SA2 at the same time while the intermediate node only obtains the IKE-SA1. The keying material calculating formulas are as follows:

(1) IKE-SA1 related:

SKEYID-1 =prf(pre-shared-key-1, Ni1 | Nm | Nr1)…… ……..….. …….. ……...….. (1)

SKEYID-d-1 =prf(SKEYID-1, g1^xyz | CKY-I | CKY-M | CKY-R | 0) ……... … .. …….. ……(2)

SKEYID-e-1 =prf(SKEYID-1, SKEYID_a-1 | g1^xyz | CKY-I | CKY-M | CKY-R | 2)…….... ….. …….. ……(3)

SKEYID-a-1 =prf(SKEYID-1, SKEYID_d-1 | g1^xyz | CKY-I | CKY-M | CKY-R | 1) … …. ….. ….…… (4)

Hash-I-1 =prf (SKEYID-1, g1^i | g1^m |g1^r | CKY-I | CKY-M | CKY-R | SA | IDi-i) ….... …….. ……..… (5)

Hash-R-1 =prf (SKEYID-1, g1^r | g1^m |g1^i | CKY-R | CKY-M | CKY-I | SA | IDi-r) .. .. …….. …..……..…...(6)

Hash-M =prf (SKEYID-1, g1^m | g1^r |g1^i | CKY-M| CKY-R | CKY-I | SA | IDi-m) .... … ..…..….. …… (7)

The pre-share-key-1 is pre-shared secret among the Initiator, Responder and PEP intermediate node. IDi-i and IDi-r are the identification payloads for the Initiator and Responder used in exchanges among three participators in phase 1 while the IDi-m is the identification payload for the PEP immediate node. CKY-I, CKY-M, CKY-R are the Initiator's cookie, the immediate node's cookie and the Responder's cookie for IKE-SA1, respectively, including in the ML-ISAKMP header (As shown in Figure 6) of messages. Hash-I-1 and Hash-R-1 are used by the PEP immediate node to authenticate the exchanges (message 12 and message 16) from the Initiator and the Responder, respectively; Hash-m is used by Responder and Initiator to authenticate the exchanges from the PEP immediate node; Hash-I-1 and Hash-I-2 are used by the PEP immediate node and the Initiator, respectively, to authenticate the exchanges from the Responder.

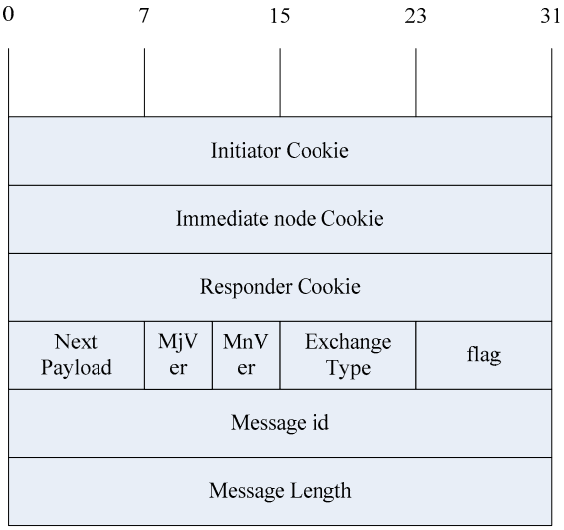

Figure 6 ML-ISAKMP Header

(2) IKE-SA2 related:

SKEYID-2 =prf (pre-shared-key-2, Ni2 | Nr2)…… ……(8)

SKEYID-d-2 =prf(SKEYID-2, g2^xy | CKY-I| CKY-R | 0)…… … ……..…(9)

SKEYID-e-2 =prf(SKEYID-2, SKEYID-a-2 | g2^xy | CKY-I | CKY-R | 2)……..(10)

SKEYID-a-2 =prf(SKEYID-2, SKEYID-d-2 | g2^xy | CKY-I | CKY-R | 1)……..(11)

HASH-I-2 =prf(SKEYID-2, g2^i | g2^r | CKY-I | CKY-R | SA | Idi-i)…… …….. …….. ……..(12)

HASH-R-2 =prf(SKEYID-2, g2^r | g2^i | CKY-I | CKY-R | SA | Idi-r)……. ……. . ……. …….. (13)

The pre-share-key-2 is pre-shared secret only between the Initiator and the Responder. Hash-I-2 and Hash-R-2 are used by the Responder and the Initiator, respectively, to authenticate the exchanges (message 13 and message 17) between each other.

3.2 Phase 2: The Quick Model of ML-IKE

The second phase is extended version of traditional quick mode, in which there are 9 messages as compared to 3 messages in traditional IKE quick mode（see figure 7）. As mentioned above, these messages are protected by the IKE-SA1 and IKE-SA2 generated in the first phase. The first 6 messages are used to exchange the parameters and key materials required to establish two suites of IPsec SAs while the last 3 messages are used to authenticate the right participators. In ML-IPsec, the first suit of IPsec SA is owned by all of the three participators and used to protect TCP header while the second suit of IPsec SA is only owned by two endpoints and is used to protect TCP payload.
When using pre-shared key encryption for authentication, Quick Mode in phrase 1 of ML-IKE is defined as Figure.7.

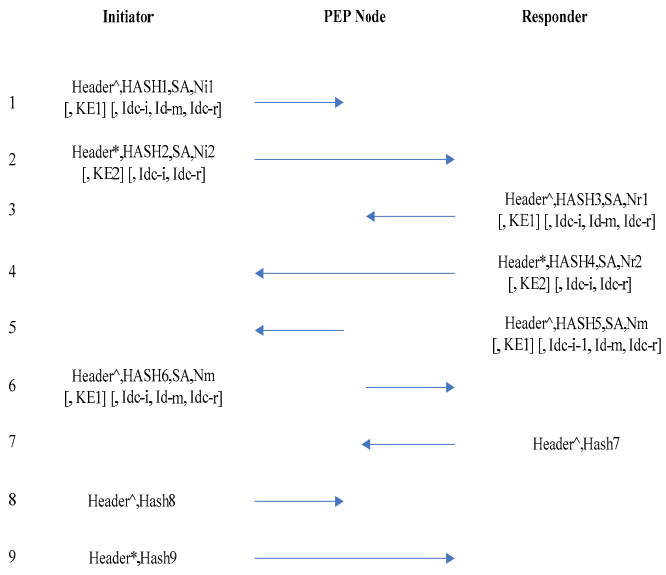

Figure.7.Exchanges of Quick Model in ML-IKE using pre-shared Key authenticate

In messages 1, 3, 5, 6, 7 and 8, the Header^ means the messages are protected by SKEYID-e-1 while in messages 2, 4 and 9 the Header* means the messages are protected by SKEYID-e-2 generated in phrase 1 of ML-IKE.

The SA Payload in message 1 can include multiple Proposal Payloads (AH and ESP) or single Proposal Payload (AH or ESP). The identities of the parties MUST be passed as IDc-i. The Responder will dictate whether the proposals are acceptable as the identities specified. If the client identities are not acceptable to the Quick Mode responder (due to policy or other reasons), a Notify payload with Notify Message Type INVALID-ID-INFORMATION should be sent to inform the quick model fails; Otherwise the responder will send message 3 and message 4 to the PEP node and the Initiator, respectively.

Message 5 and message 6 are sent by the PEP Node to the Initiator and the Responder to authenticate the PEP Node itself. Message 7 is the response from the Responder to the PEP Node while message 8 and message 9 is the responses from the Initiator to the PEP node and the Responder. The hash values for the above exchanges are as follows:

HASH1 = PRF (SKEYID_a1, M-ID | SA | Ni1 [| KE1] [| IDc-i-1 | IDc-m | IDc-r-1])……..…….(14)

HASH2 = PRF (SKEYID_a2, M-ID | SA | Ni2 [| KE2] [| IDc-i | IDc-r]) ……..……..…… . (15)

HASH3 = PRF (SKEYID_a1, M-ID | SA | Nr1 [| KE1] [| IDc-i | IDc-m | IDc-r]) ……..….. …….. ……. (16)

HASH4 = PRF (SKEYID_a2, M-ID | Ni2 | SA | Nr2 [| KE2] [| IDc-i | IDc-r]) ……..…… …… ….. (17)

HASH5 = PRF (SKEYID_a1, M-ID | Ni1 | SA | Nm [| KE1] [| IDc-i | IDc-m | IDc-r]) …….. …… … …..… (18)

HASH6 = PRF (SKEYID_a1, M-ID | Nr1 | SA | Nm [| KE1] [| IDc-i | IDc-m | IDc-r]) ……. ….. …… ….. …(19)

HASH7 = PRF (SKEYID_a1, 0 | M-ID | Nr1 | Nm) ……. ….. …… ….. … ……(20)

HASH8 = PRF (SKEYID_a1, 0 | M-ID | Ni1 | Nm) ……. ….. …….. .. ……..…(21)

HASH9 = PRF (SKEYID_a2, 0 | M-ID | Ni2 | Nr2) …….. …….. … .(22)

After the exchanges in phase 2 of ML-IKE, the negotiation of IPsec-SA1 and IPsec-SA2 is complete. The Initiator and Responder obtain the IPsec-SA1 and IPsec-SA2 at the same time while the intermediate node only obtains the IPsec-SA1. The keying material calculating formulas are as follows:

If PFS is not needed, and KE payloads are not exchanged, the new keying materials is defined as

KEYMAT1 = PRF (SKEYID-d-1, protocol | SPI1 | Ni1 | Nm | Nr1) …… (23)

KEYMAT2 = PRF (SKEYID-d-2, protocol | SPI2 | Ni2 | Nr2) ……. (24)

If PFS is desired and KE payloads are exchanged, the new keying materials is defined as

KEYMAT1 = prf(SKEYID-d-1, g1(qm)^xyz | protocol | SPI1 | Ni1 | Nm | Nr1) …… (25)

KEYMAT2 = prf(SKEYID-d-2, g2(qm)^xy | protocol | SPI2 | Ni2 | Nr2) ……. …… (26)

Where *g1(qm)^ xyz* is the shared secret from the modified Diffie-Hellman algorithm [16][17] by the three participants and *g2(qm)^xy* is the shared secret obtained by the two endpoints. The "protocol" and "SPI" are from the ISAKMP Proposal Payload that contains the negotiated Transform.

After two phases of ML-IKE negotiation, the authorized PEPs can only obtain part of key materials to access to TCP header while the two authorized endpoints can access to both TCP header and TCP payload, which means the protocol ML-IKE is suitable for ML-IPsec.

4. CONCLUSION

The end-to-end network security mechanisms such as IPsec and the rich network services such as TCP PEP for Satellite networks are two fundamental but incompatible mechanisms. ML-IPsec is just the solution for this problem. But this protocol needs a suitable key distribution protocol.

Our scheme to solve the problem is based on the layering architecture for network security protocols. The approach presented in this paper provides both security and extensibility in one unified platform.

ML-IKE is a specialized key Exchange protocol for ML-IPsec. As described above, ML-IKE is used to protect key exchanges among the endpoints and PEP while makes participators have different IPsec security associations which protect correspond IP packet fields. Through careful evaluation, ML-IKE inherits the safe attribute of traditional IKE. Through ML-IKE, the trusted PEP immediate node can obtain the IKE-SA1 and IPsec-SA1 to unencrypted (encrypt) the TCP Header but this protocol also have other mechanism using the secret only known by the legal endpoints to protect the TCP payload data from the PEP node and other illegal ponits in the network.

Through careful design, ML-IKE has the similar message format and the ML-ISAKMP is almost as same as traditional ISAKMP [15]. So in real system implement, ML-IKE is compatible with ML-IPsec and can easily be added to existing

IKE system. ML-IKE has achieved the goal of granting trusted intermediate routers a secure, controlled, and limited access to selected portions of IP datagram, while preserving the end-to-end security protection to user data.

Currently, we have done some experiments of ML-IKE approach with ML-IPsec in all-IP satellite network. Through our system implements, it shows that ML-IKE protocol is safe, efficient and suitable for layered IPsec, with ML-IKE, Multilayered IPsec is able to distribute and update key automatically.

Our plan for future work is continue to extent other models in traditional IKE such as Aggressive Mode and New Group Mode using other methods except pre-shared key encryption for authentication. Also we will investigate IKEv2 in the future to try to make IKEv2 suitable for ML-IPsec used in wireless network.

REFERENCES

1. M. Gerla, M. Luglio, R. Kapoor, J. Stepanek, F. Vatalaro, and M.A.Vázquez-Castro, "TCP via Satellite Constellations", Fourth European Workshop on Mobile/Personal Satcoms (EMPS 2000), London, September 2000.
2. Jing Zhu, Sumit Roy, and Jae H. Kim, Senior Member, IEEE, "Performance Modelling of TCP Enhancements in Terrestrial–Satellite Hybrid Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 14, NO. 4, AUGUST 2006
3. J. L. Mineweaver, J. S. Stadler, S. Tsao, and M. Flanagan, "Improving TCP/IP performance for the land mobile satellite channel," in Proc. MILCOM 2001, Oct. 2001, vol. 1, pp. 711–718.
4. Caini C , Firrincieli R . TCP hybla : A TCP enhancement for heterogeneous networks . Int'1 Journal of Satellite Journal , 2004 , 22(5) : 547-566 .
5. Luglio M , Sanadidi MY , Gerla M , Stepanek J . On—Board satellite "Split TCP" proxy . IEEE Journal on Selected Areas in Communications . 2OO4 , 22(2) : 362—370 .
6. Casetti C , Gerla M , Mascolo S , Sanadidi M , Wang R . TCP westwood : Bandwidth estimation for enhanced tran sport over wireless links . In : Basagni S , Sivalingam K , eds . Proc . ofthe MOBICoM 200l , Vo1 . 4 . Rome : lEEE Pr ess , 2001 . 54—62 .
7. Akyildiz F, Morabito G, Palazzo S. TCP-Peach: A new congestion control scheme for satellite IP networks. IEEE / ACM Trans. On Networking, 2001(9): 307—321.
8. Isci, D.D. Alagoz, F. Caglayan, M.U., IPSEC over Satellite Links: A New Flow Identification Method, Computer Networks, 2006 International Symposium on, 2006: 140-145
9. Manish Karir, John S. Baras. LES Layered Encryption Security. Center for Satellite and Hybrid Communication Networks Department of Electrical and Computer Engineering & Institute for Systems Engineering University of Maryland, College Park, MD 20742, USA
10. Y. Zhang and B. Sing. A multi-layer ipsec protocol. 9th USENIX Security Symposium, pages 113–128, Aug 2000.
11. Yongguang Zhang, Member. A Multilayer IP Security Protocol for TCP Performance Enhancement in Wireless Networks. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 22, NO. 4, MAY 2004
12. H. Fereidooni, A. Parichehreh, H. Taheri, M. Mahramian, B. Eliasi, ML-IPSec+: An End to End Accelerated VPN for Satellite Links, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.1, January 2009
13. Zhan Huang and Xuemai Gu. Design and Performance Analysis of CZML-IPSecfor Satellite Networks. K. Li et al. (Eds.): NPC 2007, LNCS 4672, pp. 277–286, 2007. © IFIP International Federation for Information Processing 2007
14. D. Harkins and D. Carrel. The Internet Key Exchange (IKE). IETF - Network Working Group, The Internet Society, November 1998. RFC2409.
15. Maughhan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.
16. Antoine Joux, A One Round Protocol for Tripartite Diffie–Hellman, Received 23 January 2003 and revised 10 June 2003 Online publication 23 June 2004

17. M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In A. De Santis, editor, Advances in Cryptology — EUROCRYPT ’94, volume 950 of Lecture Notes in Computer Science, pages 275–286. Springer-Verlag, Berlin, 1995.