ML-IKE：一种改进的卫星链路分层密钥分配协议

张亚航，程博文，文伟平
（北京大学 软件与微电子学院信息安全系，北京 102600）

摘 要：传统的IKE协议不能适用于分层IPSec协议，为了解决卫星链路中基于PEP中间节点的TCP加速技术同端到端IP安全协议IPSec之间的矛盾，本文对传统IKE主模式和快速模式进行了扩展，提出了一种改进的分层密钥分配协议：ML-IKE。该密钥分发协议用于对两端节点和中间节点分别进行密钥交换，使得不同节点具有不同安全关联SA，而不同的SA分别对应分层IPSec中不同IP包字段，因此拥有不同安全关联SA的节点具有对IP包中不同数据段的权限。ML-IKE协议适用于分层IPSec，使得分层IPSec能够进行自动的密钥分发和更新。

关键词：PEP；IKE；分层IPSec；ML-IKE
中图分类号：TP309.7 文献标识码：A

0 引言

卫星网络具有速度快，传输范围大，覆盖范围广的优点，随着宇航科技的发展，卫星传输的应用越来越广。但是卫星链路同时具有高传输延迟，较大误码率等特点。为了将地面传输网络同卫星网络实现无缝结合，提高卫星网络带宽利用率和传输效率，当前卫星链路中广泛应用了基于策略执行点（PEP）中间节点做代理网关以实现适合卫星通信的非标准 TCP 协议，如 TCP-Hybla，TCP-Westwood，PEPSal 等协议，从而达到卫星链路 TCP 加速的目的 [1-4]。

同样，在卫星网络环境中，由于卫星通信的广播特性，卫星网络的安全性问题也越来越突出。严格安全服务或协议往往实现端到端的安全特性，如 IPSec。当前越来越多的网络支持端到端的加密服务，而 IPSec 作为最常见的一种协议，在网络上得到了大量的应用 [5]。

然而，在 TCP 加速技术中，PEP 中间节点需要读写 IP 封装包中协议头信息，而这破坏了 IPSec 的端到端加密特性。因此，基于 PEP 的 TCP 加速技术同传统的 IPSec 无法兼容。为了解决基于 PEP 的 TCP 加速技术同传统 IPSec 不兼容的矛盾，美国著名卫星运营商休斯实验室 (HRL Laboratories)[6-7] 同美国太空总署 (NASA)[8] 分别独立提出了分层 IPSec 的思想，即对 IP 包数据不同的数据段进行分层处理，不同的层次对应不同的安全关联 SA 进行加密。除了两端节点具有全部的 SA，被信任的中间节点只具有该节点拥有读写权限数据段的 SA，从而达到既不破坏 IPSec 端到端安全特性，又同 PEP 兼容的目的。而哈尔滨工业大学通信实验中心在休斯实验室提出的 ML-IPSec 的基础上进行改进，提出了 CZML-IPSec，从而能够更好的支持应用层协议 HTML 等协议 [9]。

然而，这些人的研究成果不包含对分层 IPSec 协议所对应的密钥分发协议，而传统的互联网密钥分发协议 IKE 只能支持两个端节点进行密钥协商，显然无法支持分层 IPSec 协议。因此这些分层 IPSec 无法进行自动的密钥分配，只能通过人工配置密钥。本文在传统的密钥分发协议 IKE 基础上，对 IKE 的主模式和快速模式进行扩展，提出了一种分层的密钥分发协议：ML-IPSec，从而实现了对分层 IPSec 的支持。

1 分层 IPSec

由于卫星链路中基于 PEP 中间节点的 TCP 加速技术需要对 IP 包负载中的协议头部分进行读写，而传统 IPSec 的端到端安全性要求对 IP 包负载数据段进行统一的加密和完整性验证，而其对应的安全关联 SA 只有两端节点拥有。显然，TCP 加速技术中的 PEP 中间节点破坏了 IPSec 端到端的特性，两种技术无法兼容。而分层 IPSec 思想恰好能够解决这个问题。其主要思想是将 IP 数据包分为多个数据段，每个数据段对应不同的安全关联 SA 进行加密处理。如 TCP 报头采用 SA1，而 TCP 负载采用 SA2。两端节点都同时具有 SA1 和 SA2，而 PEP 中间节点只具有 SA1。因此当报文到达 PEP 中间节点的时候，该节点利用本身已存在的 SA1 对 TCP 报头进行解密，处理之后，然后再利用 SA1 重新加密，更新认证数据段。如此一来，可以实现卫星链路上的 TCP 加速功能。同时由于 PEP 中间节点不具有 TCP 负载数据段对应的 SA2，因此也无法对 TCP 负载进行解密，无法获取 TCP 负载信息，即保证了传输数据的安全性，又没有破坏 IPSec 端到端的安全特性。如图 1 所示 [5-8]。

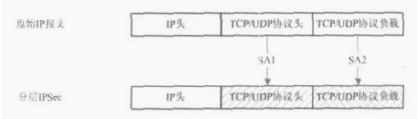

图1 分层IPSec传输模式

2 传统因特网密钥交换协议 IKE

IKE[10] 是 Oakley[11] 和 SKEME 协议的一种混合，并以 ISAKMP (Internet security association and key management protocol) 框架为基础格式运作。ISAKMP、Oalkey、SKEME 这三个协议构成了 IKE 的基础。IKE 沿用了 ISAKMP 的基础、Oakley 模式以及 SKEME 的共享密钥更新技术，从而定义出验证加密材料生成技术以及协商共享策略。

IKE 实现 IPSec 安全关联 SA 分配，主要分为两个独立的阶段：第一阶段使用主模式或者野蛮模式进行交互，用于生成 IKE SA，进而保护下一阶段的交互。传统 IKE 主模式、交互模式如下所示。

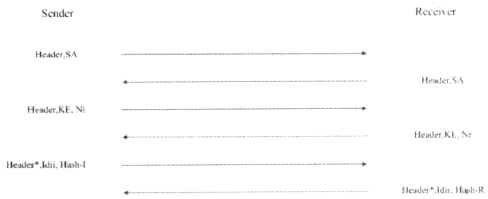

图2 共享密钥下的IKE主模式

第一阶段完成之后，两端节点完成 IKE SA 的商定。而 IKE SA 是双向的 SA，因此两端节点中的任何一个节点都可以开始第二阶段，利用第一阶段商定的 IKE SA 开始快速模式，从而建立起 IPSec SA。其具体过程如下所示。

图3 IKE快速模式

3 分层密钥分发协议：ML-IPSec

传统 IKE 能够顺利规定两端节点进行协商，从而完成为 IPSec SA 的分配。然而，传统 IKE 显然无法满足分层 IPSec 中多个节点分层安全关联 SA 的协商。通过对传统 IKE 的主模式和快速模式的扩充，我们提出并设计了分层的密钥分发协议 ML-IKE 以适用于分层 IPSec，从而为两端节点和中间节点进行分层 IPSec 多个 SA 的协商。

在卫星链路中，采用了基于 PEP 中间节点的 TCP 加速技术的卫星网络包含两端节点。为了实现端到端的安全特性，要求 IP 包在从客户端经过了公网 Internet 之后，再通过 TCP 加速，进入卫星传输，最后到达接收方，这整个过程 IP 包都是处于收到 IPSec 协议保护的状态。其网络拓扑图如下图所示。

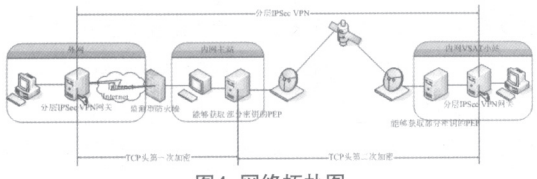

图4 网络拓扑图

在分层 IPSec 协议中，两端节点要同时拥有对 TCP 头进行加密的 SA1 和对 TCP 负载加密的 SA2。因此进行密钥协商交互的节点实际上包含三个，即发送者 sender，接收者 receiver 和中间节点 PEP。本文通过对传统 IKE 主模式和快速模式的扩充之后，形成分层密钥交换协议 ML-IKE，可以满足多个节点进行协商，完成对不同数据段不同 SA 的分配。

同传统 IKE 协议一样，ML-IKE 协议同样分为阶段一和阶段二两个阶段，其中阶段一为三个节点协商出两套 IKE SA，而这两套 IKE SA 为第二阶段快速模式服务，完成多层 IPSec 的多个数据段的 SA 协商。而第二阶段的协商，在第一阶段的 IKE SA 的保护下，完成最终的分层 IPSec SA 协商。

3.1 ML-IKE主模式：多节点第一阶段协商

在 ML-IKE 中，两端节点 Sender 和 Receiver 以及中间节点 PEP 都参与主模式协商，从而形成两套 IKE-SA。同传统 IKE 类似，这两条 IKE-SA 用来保护下一阶段的通信，并且为下一阶段 IPSec SA 提供密钥生成材料。

ML-IKE 的主模式总共拥有 17 条消息，同传统 IKE 主模式一样，分为三个回合。以基于预共享密钥的主模式为例，其具体流程如下图所示。

图5 预共享密钥的主模式流程

其中消息 1-5 属于第一回合，用于建立三个节点之间一系列安全参数共识。第一条和第二条消息内容一样，主模式中发起者的 SA 字段中包含一个提案（IKE 第一阶段），包含多个变换（表示采用的具体加密算法和散列算法）。PEP 中间节点收到第二条消息后，从多个转码中选择自己所有能支持的变换集合，即 PEP 中间节点同 Sender 所支持的变换交集，然后形成第三条消息，发送到接收者。接收者接受到第一条消息后，从中选取一个变换作为两端节点 Sender 和 Receiver 共享 IKE-SA2 的变换；接受到第三条消息之后，从第三条消息的变换集合中选取一个变换，作为两端节点和中间节点所共有 IKE-SA1 的变换。之后，分别形成第四条消息和第五条消息，其中第四条消息包含一个 IKE-SA1 的变换；而消息五将选取的两个变换放在同一个提案中，分别发送给中间节点和 Sender 节点。在本图的例子中，发起者拥有变

换 tr1,tr2,tr3；中间节点支持 tr1,tr2；接收者支持 tr2,tr3。第一回合结束后，选取 tr2 作为三个节点共有 IKE-SA2 的变换；而选取 tr3 作为两端节点共有 IKE-SA1 的变换。

消息 6-11 属于第二回合，用于完成 Diffie-Hellman 交换。Sender 节点形成两个临时值：*Ni1* 和 *Ni2*；中间节点形成一个临时值 Nm；Receiver 节点同样形成两个临时值：*Nr1* 和 *Nr2*。第七条消息和第十一条消息都包含两个 DH 形成要素。三个节点总生成三个 KE1 的 DH 公开值，通过变形的 D-H 算法，利用这三个要素形成三个节点共享的 KE1；两端节点生成两个 KE2 的 DH 公开值，通过 D-H 算法，利用这两个要素形成两端节点共享的 KE2。最后，通过这六条消息，将形成两个密钥 KE1 和 KE2，为后面的交互服务。

消息 12-17 属于第三回合，主要用于对已交换的 IKE 消息进行一致性检查和参与者的身份验证。这些消息都经过了第二回合形成的密钥进行了加密处理。其中消息 12、14、15 和 16 使用了 KE1 形成的密钥进行加密；而消息 13、17 则使用了 KE2 形成的密钥进行加密。

经过基于预共享密钥的 ML-IKE 主模式的交换，形成的 IKE-SA1 和 IKE-SA2。其中 Sender 和 Receiver 同时拥有 IKE-SA1 和 IKE-SA2，而中间节点只拥有 IKE-SA1。主模式的密钥形成材料计算公式如下：

（1） IKE-SA1 相关：

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

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

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

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

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

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

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

其中 pre-shared-key-1 是 Sender、Receiver 和 PEP 三个节点的预共享密钥。IDi-i-1 是发送者 Sender 在三节点间所用的身份信息，IDi-r-1 是接受者 Receiver 在三节点间所用的身份信息，IDi-m 是 PEP 中间节点在三节点间所用的身份信息。CKY-I-1, CKY-M-1, CKY-R-1 分别代表发起者 Sender，中间节点 PEP 和接收 Receiver 生成 IKE-SA-1 所用的 cookie 值。Hash-I-1 用于 Sender 节点生成 IKE-SA-1 的身份验证处理；Hash-m 用于对中间节点生成 IKE-SA-1 的身份验证处理；Hash-R-1 用于 Receiver 节点生成 IKE-SA-1 的身份验证处理。

（1） IKE-SA2 相关：

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

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

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

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

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

HASH-R-2=prf(SKEYID-2, g2^r | g2^i | CKY-R-1 | CKY-I-1 | SA | Idr-2).....(13)

其中 pre-shared-key-2 是 Sender 和 Receiver 两端节点的预共享密钥。IDi-2 是发送者 Sender 在两端节点间的身份信息，IDr-2 是接受者 Receiver 在两端节点间所用的身份信息。CKY-I-2, CKY-R-2 分别代表发起者 Sender 和接收 Receiver 生成 IKE-SA-2 所用的 cookie 值。Hash-I-2 用于 Sender 节点生成 IKE-SA-2 的身份验证处理；Hash-R-2 用于 Receiver 节点生成 IKE-SA-2 的身份验证处理。

3.2 ML-IKE快速模式：多节点第二阶段协商

同主模式一样，在 ML-IKE 中，两端节点 Sender 和 Receiver 以及中间节点 PEP 都参与快速模式协商，并且以第一阶段生成的 IKE-SA-1 和 IKE-SA-2 作为保护。ML-IKE 的快速模式总共拥有 9 条消息。以基于预共享密钥的主模式为例，其具体流程如下图所示。

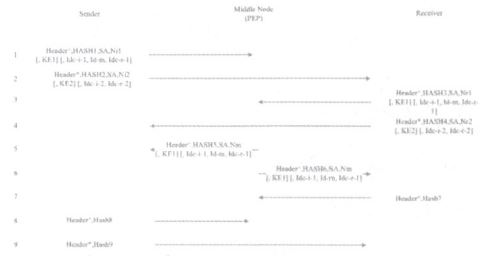

图6 预共享密钥的主模式流程

其中消息 1、3、5、6、7、8 中的 Header^ 表示其后的 Oakley 的 Header 负载采用使用第一阶段生成的 SKEYID-e-1 进行加密，而 Header* 表示其后的 Oakley 的 Header 负载采用使用第一阶段生成的 SKEYID-e-2 进行加密。

消息 1 中的 SA 载荷包含多个提案载荷 (ESP 协议 or AH 协议 or ESP AND AH 协议)，而第三条消息由 receiver 根据本地策略将决定是否接受身份指定的提案（proposal）。如果 Sender 身份没有被快速模式的响应者 Receiver 所接受（由于策略或其它原因），一个通知消息类型为 INVALID-ID-INFORMATION 的通知负载将发给 Sender 和 PEP 节点，宣告协商失败。否则，Receiver 将选择一个提案，并将已选提案通过第三条和第四条消息分别通知 PEP 中间节点和 Sender 节点。其中第四条消息同时也包含了身

份验证信息，达到 Sender 实现对 Receiver 节点验证的作用。

消息 5 和消息 6 是中间节点向两端节点进行身份验证的，而消息 7 是 Receiver 节点向 PEP 中间节点身份验证，消息 8 和消息 9 是发起者 Sender 节点分别向中间节点 PEP 和响应者节点 Receiver 证明自身身份。中间完整性保护和身份验证所用的 HASH1 到 HASH9 生成公式如下：

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-2 | IDc-r-2]).....(15)

HASH3=PRF(SKEYID_a1, M-ID | SA | Nr1 [| KE1] [| IDc-i-1 | IDc-m | IDc-r-1]).....(16)

HASH4=PRF(SKEYID_a2, M-ID | Ni2 | SA | Nr2 [| KE2] [| IDc-i-2 | IDc-r-2]).....(17)

HASH5 =PRF(SKEYID_a1, M-ID | Ni1 | SA | Nm [| KE1] [| IDc-i-1 | IDc-m | IDc-r-1]).....(18)

HASH6=PRF(SKEYID_a1, M-ID | Nr1 | SA | Nm [| KE1] [| IDc-i-1 | IDc-m | IDc-r-1]).....(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)

通过第二阶段的快速模式，IPSec SA 的密钥材料包括两套：KEYMAT1 和 KEYMAT2。其中 KEYMAT1 用于 TCP/UDP 协议头数据段的 IPSec SA，而 KEYMAT2 用于 TCP/UDP 协议负载数据段的 IPSec SA，它们的计算公式如下：

如果不考虑前向完美保密性 (PFS)，新的密钥材料定义如下 (其中两者的 protocol 是一样的)：

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

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

如果需要考虑前向完美保密性 (PFS)，新的密钥材料定义如下 (其中两者的 protocol 是一样的)：

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)

其中 g1(qm)^xyz 和 g2(qm)^xy 通过 D-H 算法和改变的 D-H 算法新协商的共享密钥。“协议”和“SPI”是从包含协商的变换（transform）负载的 ISAKMP 提议负载中得到的，所以 KEYMAT1 和 KEYMAT2 的 protocol 是一样的。

4 结论

IKE 协议的消息通信机制实现对 IPSec VPN 的密钥协商成败与否，在安全网络的设计中有着举足轻重的作用。而分层 IPSec 如果失去了密钥分配协议的支持，则在诸如卫星网络等需要中间节点处理 IP 包部分负载的应用中，无法得到推广，安全性也大大下降。本文通过对传统 IKE 主模式和快速模式的扩展，提出了分层密钥分发协议 ML-IKE，为分层 IPSec 协议的所对应密钥分发协议提供了定义，最终完善了构建卫星网络安全应用分层 IPSec VPN 的密钥分配协议部分。我们的下一步工作将为传统 IKE 野蛮模式和新组群模式等其它模式进行扩充，最终完善 ML-IKE。

（责编 杨晨）

参考文献:

[1] Caini C，Firrincieli R．TCP hybla：A TCP enhancement for heterogeneous networks．Int ' 1 Journal of Satellite Journal，2004，22(5)：P547 ～ 566．

[2] Luglio M，Sanadidi MY，Gerla M，Stepanek J．On—Board satellite " Split TCP " proxy．IEEE Journal on Selected Areas in Communications．2OO4，22(2)：P362 ～ 370．

[3] 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．P54 ～ 62．

[4] Akyildiz F，Morabito G，Palazzo S．TCP-Peach：A new congestion control scheme for satellite IP networks．IEEE／ACM Trans. On Networking，2001(9)：P307 ～ 321．

[5] 黄飞，许辉，吴诗其 . 基于 IPSec 实现卫星 ip 网的网络安全，计算机应用研究，Vol.24 No.8 Aug.2007.

[6] Y. Zhang and B. Sing. A multi-layer ipsec protocol. 9th USENIX Security Symposium, P113 ～ 128, Aug 2000.

[7] 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.

[8] 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.

[9] Zhan Huang and Xuemai Gu. Design and Performance Analysis of CZML-IPSec for Satellite Networks. K. Li et al. (Eds.): NPC 2007, LNCS 4672, pp. 277 ～ 286, 2007. © IFIP International Federation for Information Processing 2007.

[10] D.Harkins, D.carrel, The Internet Key Exchange. RFC: 2409, 1998-10.

[11] H.Orman, The OAKLEY Key Determination Protocol. RFC: 2412, 1998-10.

作者简介：张亚航 (1985－)，男，北京大学软件与微电子学院，在读硕士研究生，主要研究方向：网络安全；程博文 (1984－)，男，在读硕士研究生，主要研究方向：软件过程管理；文伟平 (1976－)，男，北京大学，副教授，主要研究方向：网络攻击与防范、恶意代码研究、信息系统逆向工程和可信计算技术等。