一种高效的 ASON 安全光路建立协议*

周贤伟，吴启武†，王建萍，王丽娜，孙勇
（北京科技大学 信息工程学院 通信工程系，北京 100083）

摘 要：针对自动交换光网络光路建立过程中存在的安全威胁，提出了一种高效的安全光路建立协议. 该协议使用综合的波长预留策略，通过数字签名和消息反馈等安全机制，对 GMPLS RSVP-TE 消息中的重要对象进行完整性保护，并可防止内部节点的恶意或自私行为. 另外，考虑到自动交换光网络中路由模块和信令模块强耦合的特点，采用 OSPF-TE 的 PKLSA 消息分发光路建立协议中所需的节点公钥证书. 经仿真实验及分析表明，该协议在保证光通路安全建立的同时，在连接阻塞率、光通路建立时间和消息负载方面都优于原有的 RSVP-TE 信令协议.

关键词：自动交换光网络；RSVP-TE；安全威胁；密钥管理；安全光路建立协议
中图分类号：TN929.11　　**文献标识码**：A　　**文章编号**：1004-4213(2009)08-2071-6

0 引言

自动交换光网络[1]（Automatically Switched Optical Network，ASON）是一种具有动态连接能力、能够支持多种类型业务、可以根据实际需求对带宽进行实时分配的光网络，它代表了下一代光网络的发展方向. 它采用 GMPLS 作为控制平面的协议体系，其中 RSVP-TE[2] 是 ITU-T 推荐的信令协议，OSPF-TE[3] 主要为连接的建立提供路由服务. 随着 DWDM 技术的发展，光网络传输的信息量十分巨大，如何安全准确地建立一条从源端到目的端之间的光通路，成了构建下一代光网络的关键问题[4].

目前，关于 ASON 信令协议安全问题的研究很少，但针对 IP 网络 RSVP 安全机制的研究已经取得了一定的进展. 例如，在 RFC 2747[5] 中提出了一种依赖于 RSVP 内在完整性对象支持的 Hop-by-Hop 保护机制，可提供完整性检测和重放保护，但它不能解决内部攻击问题且性能开销较大. Wu Tsung-li 等[6] 提出了一种 SDS/CD（Selective Digital Signature with Conflict Detection）攻击防范对策，即通过使用数字签名和完整性检测，实现对 RSVP 消息的端到端保护，它解决了 Hop-by-Hop 保护机制中不能防范的内部攻击问题. 但是 SDS/CD 没有解决重放攻击和 RESV 中 Rspec 对象的实时性反馈问题，并且缺少相应的密钥管理机制. Talwar Vanish 等[7] 提出了一种 RSVP-SQoS 安全协议，使 RSVP 消息在子网内和子网间经历不同的安全保护. 与 Hop-by-Hop 保护机制和 SDS/CD 方法相比，它是在性能上介于这两者之间的一个折衷安全解决方案，其扩展性较强但开销较大. 另外，RFC 4230[8] 对 RSVP 信令协议的固有安全属性进行了总结. Zhi Jing 等[9] 分析了 RSVP Hop-by-Hop 机制中不同的认证算法和密钥长度对连接建立时间的影响. Xia Z. Y 等[10] 解决了 RSVP 中具有不同安全处理能力的发送端和接收端之间的安全服务质量协商问题. 2008 年 IETF 公布了 GMPLS 网络安全草案[11]，该草案从用户和服务提供商的角度描述了包括信令技术在内的光网络控制平面的安全威胁和整体防范对策.

综上所述，目前针对 RSVP 协议的安全机制还不是很完善且缺少有效的密钥管理手段，也没有公开的有关专门针对 ASON 的 RSVP-TE 安全解决方案. 鉴于以上考虑，本文通过改进 SDS/CD 方法，结合优化的综合波长预留策略，提出一种高效的安全光路建立协议，对 GMPLS RSVP-TE 消息中的重要对象进行完整性保护，防止内部节点的恶意或自私等行为. 在密钥管理中，考虑到 ASON 中路由模块和信令模块强耦合的特点，使用 OSPF-TE 的相关消息分发光路建立协议中所需的节点公钥证书.

1 安全光路建立协议描述

ASON 信令协议在增加网络智能性的同时，也带来了新的安全隐患，包括主动攻击和被动攻击两大类[11]，例如未授权光标记交换路径的建立、信令消息的伪造或篡改、内部节点的自私性行为等. 针对安全光路建立协议应具有高效性的特点，本协议以波长自动交换光网络作为研究对象，采用一种综合的波长预留策略，通过改进 SDS/CD 方法，增强

* 国家高技术研究发展计划（2007AA01z213，2009AA01z217，2009AA01z209）和国家自然科学基金（60872047）资助
† Tel：010-62333498　　Email：wuqiwu700@163.com
收稿日期：2008-06-20　　修回日期：2008-09-18

RESV 中 Rspec 对象反馈的实时性. 为了描述方便，我们将安全光路建立协议简称为 SLEP(Secure Lightpath Establishment Protocol). 下面分别对 SLEP 中的波长预留策略、密钥管理过程、安全光路建立过程进行描述.

1.1 波长预留策略

波长预留策略大致可分为前向波长预留和后向波长预留两大类. 针对这两类预留策略的不足，目前有人提出了综合的波长预留策略[12-15]，这种策略充分利用了前向预留和后向预留的优点，性能较为理想. SLEP 通过改进现有的综合波长预留策略，入口节点使用一定的算法开始尝试预留空闲波长集合中的某个波长，如果到下游节点发现此波长仍然可用，继续保持预留. 一旦发现此波长被占用，中间节点则向各上游节点发送信令消息来取消相应波长的预留，为其它的连接请求提供更多的波长资源预留机会，然后重新按照后向波长预留过程处理，且在此过程中不再做其他波长的预留.

1.2 密钥管理过程

密钥管理作为一种技术和过程，它能够在光网络节点间提供密钥关系的建立和维护. SLEP 协议使用基于公钥基础设施(Public Key Infrastructure, PKI)的密钥管理方案，其中主要的密钥管理过程描述如下：

1)密钥产生阶段. 在本协议中，每个光网络节点按照数字签名算法产生自己所需的公钥和私钥. 并向证书机构(Certificate Authority，CA)申请 CA 签名的公钥证书，以保证公钥的真实性.

2)密钥分发阶段. 考虑到 ASON 中路由模块和信令模块强耦合的特点，我们利用 OSPF-TE 路由协议的特点，采用 PKLSA(Public Key Link State Advertisement)类型[16]的报文来分发每个节点的公钥证书，公钥证书到达每个节点后，如果对 CA 的签名验证通过，节点将此证书保存至该节点的公钥数据库中.

3)密钥更新阶段. 在密钥更新中，采用定时更新和事件激活相结合的方式来引发相关密钥更新操作. 例如，可根据系统安全强度的需要来设定密钥更新定时器的更新时间间隔值.

4)密钥存储阶段. 我们设计了一种类似数据库的 PublicCertMap 的数据结构来存储收到的每个节点的公钥证书，利用它可以灵活地删除、插入、查找、更新证书. 对私钥采取加密和保护存储.

1.3 安全光路建立过程

安全光路建立协议 SLEP 利用攻击预防和入侵检测的原理，对 RSVP 消息中的不变对象进行数字签名及验证，使用消息反馈机制对 Adspec 和 Rspec 等重要可变 QoS 对象实施对节点的恶意或自私行为检测，下面对 SLEP 过程进行简要描述.

1)波长交换网络的入口节点(Ingress Node)接收到来自客户网络的连接请求以后，计算显示路由和确定空闲波长，并用本节点的私钥对 PATH 消息中的恒定不变对象如序列号 Number、业务流特征参量 Tspec 等进行数字签名，并将与描述 QoS 相关的 Adspec、空闲波长集合、显示路由等可变对象封装在 PATH 中. 在将 PATH 消息发往下一个节点的同时，按照一定的算法从空闲波长集合中选出一空闲波长 λ^* 进行预留，并对已经预留的波长 λ^* 作特定标记.

2)当中间节点收到 PATH 消息后，执行下面的攻击检测与波长预留算法. 其中，对 PATH_ERR 消息也实施类似的数字签名保护.

```
BEGIN  /* 算法开始 */
IF (Find-PublicKey (NodeID) =TRUE) THEN
PK=Find-PublicKey (NodeID);
ELSE
GOTO LABEL;
END IF
IF Message sequence is not new THEN
GOTO LABEL;
END IF
IF (Verify-Signature (PATH, PK) = TRUE) THEN
/* 波长预留策略开始 */
L S= Receive Label Set ∩ Node Label Set;
IF λ* is free in L S THEN
Reservation λ* Successfully;
ELSE
Send PATH ERR to up node for wavelength release;
END IF
Update PATH QoS Object like Adspec;
Forward PATH Message to down node;
/* 波长预留策略结束 */
ELSE
GOTO LABEL;
END IF
LABEL:
Send security warning to local PDP
Decide whether send PATH ERR and terminate the
LightPath Setup or not;
END /* 算法结束 */
```

其中，Find-PublicKey() 表示在本地数据库中查找公钥，Verify-Signature() 表示数字签名验证.

3)当出口节点(Egress Node)收到 PATH 消息后，执行 2)中的攻击检测过程. 若检测通过，出口节

点继续判断特定波长 λ^* 是否空闲，若 λ^* 空闲，则选择此波长进行交叉连接操作，否则出口节点选择一个空闲波长开始交叉连接操作. 最后，出口节点使用自己的私钥对 Adspec(PATH)、空闲波长、Rspec 等不变对象进行数字签名，然后封装在 RESV 消息中，向出口节点方向发送.

4)当中间节点收到此 RESV 消息后，除了先执行 2)中类似的攻击检测之外，同时检测收到的 Adspec(PATH)对象值是否等于或小于自己转发给下游的封装在 PATH 消息中的 Adspec(PATH)对象值，因为过大的 Adspec 很可能是攻击节点的引诱行为. 若检测通过且 RESV 指示的波长空闲，中间节点将使用已经预留的波长或携带的空闲波长进行交叉连接操作. 若指示的波长已占用或交叉连接失败，中间节点则向出口节点方向发送 RESV ERR 消息，通知出口节点此波长的连接建立失败，同时告知返回路径上的其它节点进行相关资源的释放.

5)在中间节点处，若当一个流有多个接收者且多个接收者到发送者的路径汇集在一起时，可以把这些接收者的所要求的预留参量合并起来，即合并多个 RESV 消息，那么这个中间节点应将挑选出一个 Rspec(RESV)值最大的 RESV 消息，并转发给上游节点，并进行合并标识.

6)当 RESV 消息到达入口节点后，先执行与 4)中的类似攻击检测过程. 若攻击检测通过且不存在预留合并的情况，那么此次光通路已经安全的成功建立. 若验证通过且存在预留合并的情况，入口节点先利用建立好的光通路进行数据的传输，然后利用本节点的私钥对收到的 Rspec(RESV)和其它不变对象进行数字签名，封装在 RESV_CONFIRM 消息中，并赋予此类 RESV_CONFIRM 消息以较高的转发优先权. 中间节点收到此类消息后，对 RESV_CONFIRM 消息进行 2)中的类似的攻击检测，并比较收到的 Rspec(RESV)对象值是否大于或等于自己转发给上游的封装在 RESV 消息中的 Rspec(RESV)对象值. 若检测未通过，则发送警告消息给本地的策略决定中心，由其来确定是否丢弃此 RESV_CONFIRM 消息或发送连接拆卸的 Tear 消息. 若检测通过，则继续转发，直至出口节点.

图 1 为综合波长预留策略下安全光路建立示意图. 其中，λ^* 在节点处被占用，然后启动后向预留过程. 其中 RESV_CONFIRM 的发送由是否存在预留合并决定.

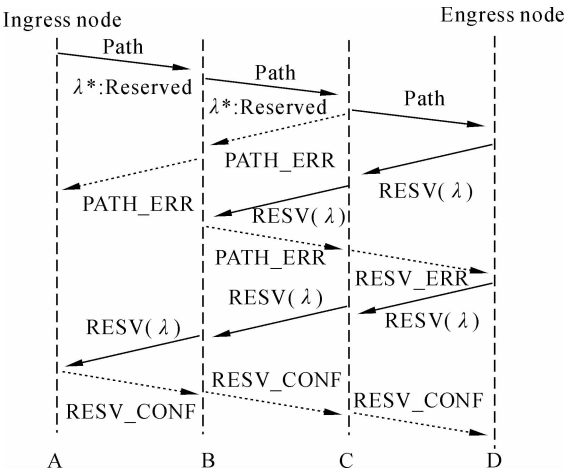

图 1　安全光路建立过程

Fig. 1　Secure lightpath establishment process

2　安全光路建立协议分析

下面将对 SLEP 协议的安全性、时间复杂度和消息复杂度进行分析.

1)安全性分析

①完整性保护. SLEP 通过对消息中不变对象的消息摘要进行数字签名及验证，检测来自外部和内部的消息篡改攻击，进行消息完整性保护.

②防止内部节点的恶意行为. SLEP 使用了对重要可变对象实施反馈比较的机制，防止内部节点对重要 QoS 参量的恶意篡改，保证客户网络获得希望的服务.

③重放保护. 通过递增消息序列号的使用，可防止 RSVP-TE 消息的重放攻击.

④防止伪造消息. 协议使用了基于数字签名的消息源认证机制，可确认消息来自正确的发送方.

2)复杂度分析

(1)时间复杂度

设 N 为 ASON 中的节点个数，n 为内部恶意节点(修改可变对象)距离入口节点的跳数，L 为 PATH 消息中空闲波长的个数，T_t 为网络中经历一跳所需的平均时间，T_p 为节点内部前向处理和后向处理过程的平均处理时间，包括数字签名、波长预留、光交叉连接建立或配置等. 为了简单起见，这里假设节点的数字签名过程及签名验证过程的所需时间相同. 这样，一个光通路建立所需时间 T 为消息传输时间和消息处理时间之和.

①光通路建立时间. SLEP 的光通路最短建立时间 $T=(2\times N-2)\times T_t+(2\times N-1)\times T_p$，即一次信令发起和响应过程可成功完成光路的建立. 光通路最长建立时间 $T=(2\times N-2)\times T_t+(2\times N-1)\times T_p+(N-2)\times 2\times(L-2)\times T_t+(N-2)\times 2\times(L-2)\times T_p=(4\times N\times L-2\times N-4\times L+6)\times$

$T_t+(4\times N\times L-2\times N-4\times L+7)\times T_p$.

②攻击检测时间. 设 n 为篡改可变对象的恶意节点距离入口节点的跳数. 若恶意节点篡改可变对象的内容,则攻击检测时间 $T=(2\times N-n-1)\times T_t+(2\times N-n)\times T_p$,即当反馈消息到达恶意节点的前一个节点后,便可以检测出恶意节点的非法篡改行为. 若恶意节点篡改不变对象的内容,则攻击检测时间 $T\leqslant T_t+T_p$,即在下一个节点的攻击检测过程中便可检测出此攻击.

因为 T_t 和 T_p 均为统计后的平均时间,即为常量,所以 SLEP 光通路建立的时间复杂度和攻击检测的时间复杂度均为 $O(N)$,其中 N 为网络中节点个数.

(2)消息复杂度

由于 SLEP 充分利用了原有 RSVP-TE 信令协议的消息及过程,没有增加额外的信令消息,只是对信令消息进行了扩展,所以在信令基本协议部分,与原来的 RSVP-TE 相比,其消息复杂度保持不变. 但在所需的相关密钥管理中,本协议使用了 OSPF-TE 路由协议的 PKLSA 报文,由于 PKLSA 利用了 OSPF-TE 消息泛洪的特点,这样网络中 PKLSA 消息交换的复杂度至多为 $O(N^2)$,其中 N 为网络中节点的个数. 尽管其消息交换复杂度为非线性级的,但由于 PKLSA 的发送由事件或定时器驱动控制,所以这对于可保证光路安全建立的光网络来说,如此的消息复杂度是可以接受的.

3 实验与结果分析

3.1 实验设置

为了验证协议的有效性,我们使用 NS-2[17] 搭建了一个 ASON 仿真平台,SLEP 协议在 GMPLS RSVP-TE 上扩展实现,路由协议采用 GMPLS OSPF-TE,并在其上添加了 PKLSA 报文. 另外,采用离线的方式为每个节点配置 CA 签名的公钥证书. 仿真采用中国教育科研网 CERNET 作为拓扑结构,光连接请求到达满足泊松分布,连接保持时间满足指数分布,网络负载的单位为爱尔兰(Erlang). 各节点之间的光纤链路上的波长数为 16,波长的带宽为 2.5Gbps. 网络同时设置 2 个攻击节点分别执行伪造信令消息和篡改重要 QoS 参量的恶意行为.

3.2 实验结果及分析

基于上述网络设置,我们仿真了 SLEP 和使用固有安全机制的 RSVP-TE 在连接阻塞率、光通路建立时间、信令消息负载上的性能. 仿真结果中每个样点是平均 1500 个连接建立过程的结果.

1)连接阻塞率

图 2 给出了 SLEP 和 RSVP-TE 平均连接阻塞率随着网络负载变化的曲线. 可以看出,随着网络负载的增加,两种安全协议的连接阻塞概率都在上升,但是 RSVP-TE 引起的平均连接阻塞率明显高于 SLEP. 一方面,这是因为 RSVP-TE 中内部恶意节点对连接的 QoS 参量进行了篡改,使连接因为 QoS 得不到保证或费用太高而引发阻塞. 另一方面,在网络资源合理利用上,SLEP 的波长混合预留策略比 RSVP-TE 原有的后向空闲波长直接使用策略更优,减小了因波长资源缺乏而引发连接阻塞的概率.

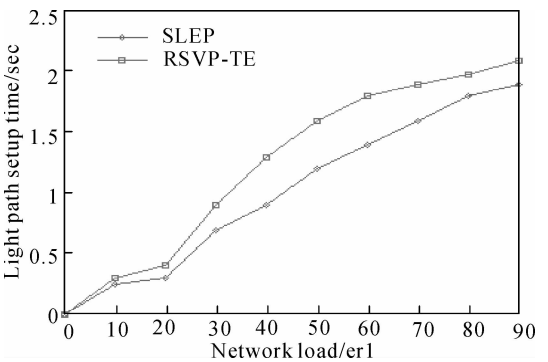

图 2 连接阻塞率与网络负载的关系

Fig. 2 Blocking probability and network load

2)光通路建立时间

图 3 给出了 SLEP 和 RSVP-TE 对光通路建立时间的影响. 可以看出,随着网络负载的增加,两种安全协议的平均光通路建立时间都在上升,但 SLEP 的平均光路建立时间比 RSVP-TE 要短. 这是主要是因为 RSVP-TE 的 Hop-by-Hop 保护机制带来的处理开销比 SLEP 要大.

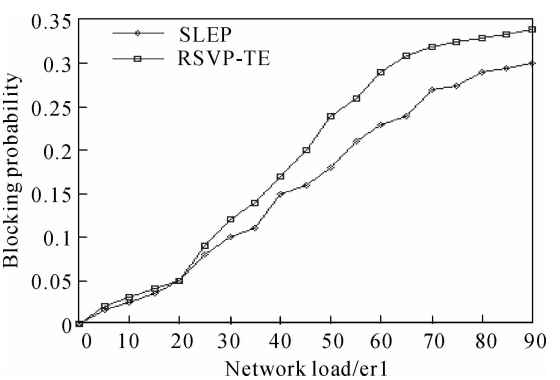

图 3 光路建立时间与网络负载的关系

Fig. 3 Lightpath setup time and network load

3)信令消息负载

图 4 给出了 SLEP 和 RSVP-TE 的信令消息负载. 可以看出,在刚开始时 SLEP 的消息量要略高于 RSVP-TE,这是因为运行初期,SLEP 增加了密钥管理所需的 PKLSA 消息和相关的 ACK 报文. 但随着运行时间的变长,空闲波长资源逐渐变少,RSVP-TE 后向重试操作的可能性更大,即一个连接建立成功可能包含了更多的 RESV 过程,所以 RSVP-TE 的消息负载高于 SLEP.

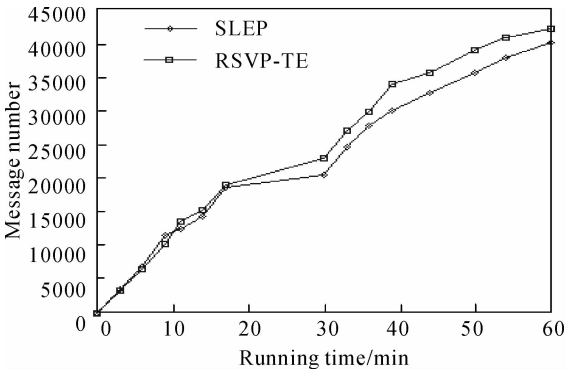

图 4　运行时间与信令消息数目的关系

Fig. 4　Message number and running time

4　结论

针对 ASON 光通路建立过程中可能存在的安全威胁，本文在深入研究现有方法的基础上，通过改进 SDS/CD 方法，提出了一种光网络安全光路建立协议 SLEP. 经仿真及分析可知，与使用固有安全机制的 GMPLS RSVP-TE 相比，运行 SLEP 的波长交换网络具有较低的连接阻塞概率、较短的光通路建立时间，同时控制网络也具有较低的消息负载.

参考文献

[1] ITU-T Recommendation G8080/Y1034. Architecture for the automatically switched optical network (ASON)[S], 2001.

[2] BERGER L. Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions[S]. IETF RFC 3473, January 2003.

[3] KATZ D, KOMPELLA K, YEUNG D. Traffic Engineering (TE) Extensions to OSPF Version 2 [S]. RFC 3630, September 2003.

[4] MANNIE E. Generalized Multi-Protocol Label Switching (GMPLS) Architecture [S]. RFC 3945, May 2002.

[5] BAKER F, LINDELL B, TALWAR M. RSVP Cryptographic Authentication[S]. RFC 2747, January 2000.

[6] WU T L, WU S F, GONG F M. Securing QoS: Threats to RSVP Messages and Their Countermeasures[C]. *Proc of IWQoS*, *IEEE*, **1999**, 62-64.

[7] TALWAR V, NAHRSTEDT K, GONG F. RSVP-SQOS: a secure RSVP protocol [C]. *Proc of IEEE International Conference on Multimedia and Expo* (*ICME*2001), *Tokyo*, **2001**, 579-582.

[8] HANNES T, RICHARD G. RSVP Security Properties[S]. RFC 4230, 2005.

[9] ZHI J, LUNG C H, XU X, *et al*. Securing RSVP and RSVP-TE signaling protocols and their performance study[C]. *Proc of Information Technology Research and Education*, *IEEE*, **2005**, 90-94.

[10] XIA Z Y, HU Y A. Extending RSVP for quality of security service [J]. *IEEE Internet Computing*, 2006, **10**(2): 51-57.

[11] FANG L, BEHRINGER M, CALLON R, *et al*. Security Framework for MPLS and GMPLS Networks[S]. draft-ietf-mpls-mpls-and-gmpls-security-framework-02.txt, February 2008.

[12] DENG Yu, ZHAO Lei, XIE Jie-lan, *et al*. Research of Resource Reservation Schemes of RSVP-TE in ASON[J]. Acta Photonica Sinica, 2007, **36**(10):1849～1852.
邓宇，赵蕾，谢洁岚，等. ASON 信令协议 RSVP-TE 中资源预留策略研究[J]. 光子学报，2007，**36**(10):1849-1852.

[13] LIU ji-min, ZENG Qing-ji, LUO Xuan, *et al*. An efficient signaling protocol for distributed-controlled optical network [J]. *Acta Photonica Sinica*, 2004, **33**(9):1104- 1107.
刘继民，曾庆济，罗萱，等. 分布式控制光网络的一种高效信令协议[J]. 光子学报，2004，**33**(9):1104-1107.

[14] PAN Deng, QI Zhi-gang, ZHAO Ji-jun, *et al*. A new dynamic wavelength assignment algorithm: load equalization algorithm [J]. *Acta Photonica Sinica*, 2003, **32**(6): 710-713.
潘登，齐志刚，赵继军，等. 一种实现负荷均衡的动态波长分配新算法[J]. 光子学报，2003，**32**(6):710- 713.

[15] SUN Wei-qiang, HONG Pei-lin, LI Jin-sheng, *et al*. CLEP-A new lightpath establishment protocol in all optical networks[J]. *Acta electronica sinica*, 2004, **32**(2): 254-258.
孙卫强，洪佩琳，李津生，等. CLEP ——一种新的全光网络光路建立协议[J]. 电子学报，2004，**32**(2): 254-258.

[16] MURPHY S, BADGER M, WELLINGTON B, OSPF with Digital Signatures [S]. RFC 2154, June 1997.

[17] Network Simulator 2 [EB/OL]., http://www.isi.edu/.

An Efficient Secure Lightpath Establishment Protocol in ASON

ZHOU Xian-wei, WU Qi-wu, WANG Jian-ping, WANG Li-na, SUN Yong
(*Department of Communication Engineering, School of Information Engineering, University of Science and Technology Beijing, Beijing* 100083, *China*)

Abstract: To the point of security threats against lightpath establishment process in ASON, an efficient secure lightpath establishment protocol is presented. This protocol uses integrated strategy of wavelength reservation, and makes use of digital signature and message feedback security mechanisms to protect the integrity of important object in GMPLS RSVP-TE message and prevent malicious or selfish actions from inner node. In addition, in view of the close coupling character of routing and signaling module in ASON, this protocol adopts PKLSA message of OSPF-TE to distribute node's public key certificate which the lightpath establishment protocol demanded. Through simulation experiment and analysis, it is proved that this protocol can ensure the security of lightpath establishment, and has better performance than the old RSVP-TE protocol in terms of connection block probability, lightpath connection setup time and message overhead.

Key words: ASON; RSVP-TE; Security threat; Key management; Secure lightpath establishment protocol.

ZHOU Xian-wei obtained the Ph. D. degree from Southwest Jiaotong University. He was engaged in postdoctor study at School of Electronic and Information Engineering of Beijing Jiaotong University. Now, as a professor of University of Science and Technology Beijing, his research interests include the security of communication networks, next generation networks, scheduling theory, and game theory.