

等级 OSPF 网的安全保护方案

孔令晶*, 曾华燊, 李 耀

(西南交通大学 信息科学与技术学院, 成都 610031)

(* 通信作者电子邮箱 kafeishunzi@163.com)

摘 要: 开放式最短路径优先(OSPF)协议作为目前大规模网络应用最广泛的自治域内路由协议,其安全不仅仅关系到自治域内,同时也关系到自治域外乃至整个网络的正常运行。传统的基于非对称性加密算法的数字签名解决方案能够实现端到端的安全验证,但是却忽略了点对点的方式,而且存储量和额外开销也一直是急需解决的问题。基于对称性加密算法,提出了适宜于 OSPF 等级区域的安全防护方案 HS-OSPF。HS-OSPF 扩充了 OSPF 网原有的二层等级结构,设计了合理、高效的密钥分配与管理方案,克服了传统非对称性密码方案的不足,降低了密钥存储量和系统开销,提高了网内安全通信的实时性。

关键词: 开放式最短路径优先协议;自治域内;对称加密算法;等级结构;存储量;实时性

中图分类号: TP393.08 **文献标志码:** A

Secure protection scheme for hierarchical OSPF network

KONG Lingjing*, ZENG Huashen, LI Yao

(School of Information Science and Technology, Southwest Jiaotong University, Chengdu Sichuan 610031, China)

Abstract: As the most widely used autonomous intra-domain routing protocol for large-scale network, the security of Open Shortest Path First (OSPF) is not only about the normal running of autonomous intra-domain, but also closely related to inter-domain even the whole network. Based on asymmetric encryption algorithm, the traditional digital signature solution can realize the security validation of end-to-end; however, it ignores the issue of point-to-point. Additionally, the problem of storage and extra overhead also needs to be solved urgently. On the basis of symmetrical encryption algorithm, a new solution named HS-OSPF was put forward. HS-OSPF extended the original two-level hierarchical structure as well as designed a reasonable, efficient key distribution and management scheme. The result shows that the shortcomings of traditional solution are overcome, key storage and system overhead are reduced and real-time of security communication is improved.

Key words: Open Shortest Path First (OSPF) protocol; intra-domain; symmetrical encryption algorithm; hierarchical structure; storage; real-time

0 引言

网络中的路由器通过路由方式将信息从源地点传递到其他目的地,从而连通世界的每个角落。不同的一组组路由器和网络群组成了各自的自治系统(Autonomous System, AS),并在统一的管理机制下通过路由协议交换路由信息。著名的边界网关协议 BGP-4 (Border Gateway Protocol)^[1] 承担了 AS 之间的信息传递;而自治系统内部,则利用内部网关协议 (Internal Gateway Protocol, IGP) 来传递路由信息,例如路由信息协议 (Router Information Protocol, RIP)^[2], 开放式最短路径优先 (Open Shortest Path First, OSPF)^[3] 协议和中间系统到中间系统 (Intermediate System to Intermediate System, IS-IS) 路由协议^[4]。OSPF 是使用最为广泛,且更适合于大规模网络的内部网关路由协议。目前使用的 OSPF v2 从 1998 年出现一直沿用到现在,不仅仅在 AS 内部的网络通信中担任着重要的角色,而且通过 BGP 发言者能够影响 AS 外部的路由信息交换。然而路由器节点作为 OSPF 网络中的公开实体,非常易于遭受攻击者的侵袭,从而影响局部网络甚至是整个网络的正常运行。

从攻击者的来源来看,攻击者可以分为内部攻击者和外部攻击者^[5]。内部攻击者是指攻击者本身已被视为参与路由信息交换的可信实体(合法路由器),这个实体可以通过任何方式获得 OSPF 网络身份认证的共享密码的实体,也可以是由于本身的配置或操作错误所致的具有安全漏洞的实体。外部攻击者则不是路由信息交换的参与者,也不持有身份认证的共享密钥。外部攻击者能够通过窃听路由信息获取网络的拓扑结构,假冒成合法的参与者注入错误路由信息或利用不断重发导致拒绝服务 (Denial of Service, DoS) 等方式对 OSPF 网络造成威胁。而内部攻击者由于其本身已被视为合法的成员,所以可以更容易假冒成其他路由器发布错误信息。肆意篡改路由引入错误的信息,泄露信息或者发起 DoS 攻击等也都是内部攻击者经常使用的手段。

保证网络的安全性,其实就是保证网络信息的机密性 (confidentiality)、完整性 (integrity) 以及可用性 (availability)。机密性是指防止将信息泄露给未被授权的合法实体;完整性包括了数据源的真实性以及信息内容的完整性,即数据源是否真实可信,且传输过程中是否遭受肆意篡改;可用性是指被授权的合法实体能否及时获取所需信息并使用的能力。最为

收稿日期:2013-02-04;修回日期:2013-03-30。

基金项目:国家自然科学基金资助项目(60773102);国家自然科学基金与中国工程院联合基金资助项目(U0970122)。

作者简介:孔令晶(1983-),女,甘肃兰州人,博士研究生,主要研究方向:下一代网络安全;曾华燊(1945-),男,四川成都人,教授,博士生导师,主要研究方向:下一代网络体系结构、高速交换、网络测试;李耀(1985-),男,四川南充人,博士研究生,主要研究方向:安全苛求系统可靠性与安全性。

熟知的 DoS 攻击就是破坏网络可用性的手段之一。针对可用性大多采取的解决方案都是被动性的入侵检测系统 (Intrusion Detection System, IDS) 和防御系统等。本文所提出的 OSPF 安全解决方案是基于对称性密码算法的主动防御方案,着重讨论信息的机密性和完整性,达到防止攻击者获取网络信息和操控路由的目的。

1 相关工作

OSPF 自诞生以来,就其安全漏洞已经出现了一系列相关解决方案。OSPF v2 本身设计的认证机制——哈希消息认证码 (Hashed Message Authentication Code, HMAC)^[6-7] 通过单项哈希函数从 OSPF 协议包和共享密钥计算相应的摘要,并追加在协议包尾部。HMAC 能够防止攻击者对信息的伪造和篡改,从而保证信息的完整性。但是这种认证机制并不能够保证信息的机密性,完整性方面也仅仅是实现了端到端的方式,而忽略了点到点的方式。1997 年文献[8]提出了基于数字签名的安全解决方案,利用非对称性密码学理论保证信息的机密性和完整性。文献[9-10]也是基于数字签名技术的 OSPF 安全方案,但这些方案仅仅停留于端到端的方式,并存在着系统计算开销、通信实时性以及存储量等问题。由于非对称性密码方案的局限性,随后很多学者将注意力转向了对称性密码学理论,如文献[11-12]。然而到目前为止,针对 OSPF 网络的区域间的等级结构并没有提出高效的、低存储量且高实时性的解决方案。

本文基于对称性密码学,提出新的安全解决方案——HS-OSPF (Hierarchical Secure-OSPF)。此方案将 OSPF 网的二层等级结构扩充为三层等级结构,并利用分布式密钥管理机制建立了多层次、多区域的安全模型,实现了高效的密钥分配与管理,同时也保证了层次之间以及区域之间的安全通信。与传统方案相比,不仅降低了存储量的需求,同时也降低了系统开销,提高了安全通信的实时性。

2 OSPF 协议及等级结构

2.1 OSPF 协议

OSPF 网络中的每个路由器借助连接状态宣告 (Link State Advertisement, LSA) 将本身的接口和邻接状态洪泛到整个路由域内,使得路由域内的每个路由器都拥有完全相同的连接状态数据库,并通过连接状态库使用最短路径优先 (Shortest Path First, SPF) 算法生成以自己为根节点的最短路径树,最终生成路由表,实现路由选择和信息转发^[3]。每个路由器可以生成一条或几条 LSA,假设 OSPF 网络中共有 n 个路由器,则至少会产生 n^2 条 LSA。随着网络规模的扩大,将会产生更多的 LSA,更频繁的 SPF 计算以及更大规模的路由表^[13],很显然,这些因素直接地影响了网络的性能。

针对于此,OSPF 允许将 AS 划分为一系列小规模“区域 (Area)”。这些区域拥有各自的连接状态数据库,并独立运行着各自的连接状态路由算法。每个区域的拓扑结构对外是不可见的,而区域内的路由器也不清楚区域外的拓扑细则。通常区域内的数据包仅转发区域内的路由信息,而不涉及区域外的相关信息。在某种程度上,区域的划分保护了区域内部免受外部错误信息的侵害。

2.2 区域间的等级结构

基于“区域”的概念,OSPF 网络具有如图 1 所示的等级结构特性^[13]。

每个区域都会授予唯一的区域号,区域号按照 IP 地址的

格式 $x.x.x.x$ 标记。其中 OSPF 的特殊区域——骨干区域被记为 $0.0.0.0$,记为 $Area_0$ 。骨干区域负责传递不同区域间的路由信息,这个概念类似于 AS 级网络中的骨干网。其他区域可以依次记为 $Area_1, Area_2, \dots$ 。区域边界路由器 (Area Border Router, ABR) 承担了连接不同区域的重任,负责将其所连接非骨干区域的拓扑信息进行汇总,再通过骨干区域发布给其他区域的 ABR。如果一条路由信息要从 $Area_1$ 转发到 $Area_2$,如图 1 所示,需要经历: $Area_1 \rightarrow Area_0 \rightarrow Area_2$ 三个阶段。很显然,骨干区域在整个 OSPF 网络中占据了主导地位。

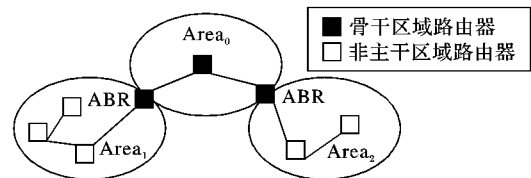


图1 OSPF 等级结构

HS-OSPF 将 OSPF 网本身的二等级结构扩充为三层等级结构,增加了位于最高层的 $Level_1$,即密钥管理中心 (Key Management Center, KMC),负责 OSPF 主干区域的密钥、身份标识以及它们之间关系的预分配。其余层次向下依次是 $Level_2$ (骨干区域) 和 $Level_3$ (除骨干区域以外的普通区域)。金字塔形的等级结构如图 2 所示。

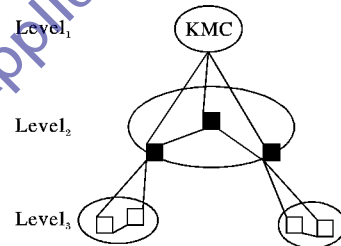


图2 金字塔等级结构

二等级结构的扩充使得密钥管理不仅仅只集中于 KMC,而是分布于 $Level_2, Level_3$ 的密钥管理将不再依赖于 KMC。扩充后的结构将 KMC 的密钥管理开销分摊给了 $Level_3$ 的密钥管理者,减少了 KMC 的管理负担,提高了密钥管理效率,同时也降低了存储量需求。然而这种方式也存在了不足之处: $Level_3$ 对 $Level_2$ 的信任并没有完全的安全保障。即便 $Level_2$ 本身的防御能力可以抵制部分敌人的攻击,但是一旦被强大的敌人侵入,不仅仅会直接影响到所管辖的局部区域内的所有成员,甚至会殃及其他区域乃至整个网络。所以考虑在 $Level_2$ 部署额外的攻击检测及防御系统,尽可能对敌人的入侵做到及时响应与防御,从而控制威胁的大面积蔓延。

3 安全解决方案

3.1 基于单向哈希函数的密钥链生成

3.1.1 单向哈希函数及其性质

在现代密码学中单向哈希函数 (One-way Hash Function) 是对称性密码解决方案的重要组成部分。

哈希函数具备如下特殊性质^[14]:

- 1) 输入:任意长度的 x ;输出:固定长度的 $y = h(x)$ 。
- 2) 快速性:给定输入 x 、哈希函数 h ,能够很容易计算出输出 $y = h(x)$ 。
- 3) 单向性:对于给定的输出 $y = h(x)$,要想找到哈希值等于 y 的输入在计算上是不可行的,即给定任意的 y ,找到 x ,使得 $y = h(x)$ 是不可行的。
- 4) 弱无碰撞:对于任意确定的输入,要找到任何一个与

它有同样输出的另外一个输入在计算上是不可行的,即对于一个确定的 x_1 ,要找到另外一个 x ,使得 $x_1 \neq x$,且 $h(x_1) = h(x)$ 在计算上是不可行的。

5) 强无碰撞: 要找到两个不同的输入 $x_1 \neq x$,使得 $h(x_1) = h(x)$ 在计算上是不可行的。

3.1.2 哈希链及其性质

哈希链^[15]: 选择一个哈希函数 h , 并选择一个密钥种子 sd , 迭代哈希函数 h 共 n 次, 生成一个哈希链, 链尾 $h^n(sd)$ 记为 t , 如下所示:

$$t = h^n(sd) = h(h^{n-1}(sd)) = h(h^{n-2}(h(sd)))$$

哈希链具有如下特殊性质:

- 1) 当 $j_2 > j_1 \geq 0$, 给定 $h^{j_2}(sd)$, 无法推出 $h^{j_1}(sd)$;
- 2) 当 $j_2 > j_1 \geq 0$, 在 $h^{j_1}(sd)$ 可信的前提下, 可通过验证等式 $h^{j_2}(sd) = h^{j_2-j_1}(h^{j_1}(sd))$ 判断 $h^{j_2}(sd)$ 是否可信。

3.1.3 密钥链的生成与分配

基于哈希函数和哈希链的理论, 选取 $sd_i (i = 1, 2, \dots, n)$ 作为密钥种子(即根密钥), 通过迭代生成密钥链。假设 h 为Hash函数, f 为密钥生成函数, m_i 为区域内的合法成员(合法的路由器), 那么初始密钥 $k_{i0} = f(sd_i)$ 。根据哈希链的迭代性质, 可以得到:

$$\begin{aligned} k_{i1} &= h(k_{i0}) \\ k_{i2} &= h(k_{i1}) = h^2(k_{i0}) \\ &\vdots \\ k_{in} &= h(k_{i(n-1)}) = h^2(k_{i(n-2)}) = \dots = f(h^n(k_{i0})) \end{aligned}$$

哈希密钥链生成与分配图如图3所示, 链中的每个元素 k_{ij} 分别分配给不同的路由器成员^[16]。

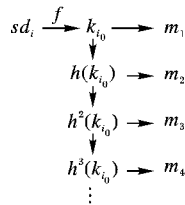


图3 密钥链生成与分配示意图

可以看出, 哈希密钥链从上到下, 高等级的密钥可以计算出低等级的密钥, 反之则不可行。

定义1 通信组。指一个发送方与多个接收方通信而组成的临时群组。通信组的每个成员仅持有密钥链的一个元素, 且以持有初始密钥 k_{i0} 的成员为基准, 依次顺序从上到下与其他连续相邻成员结合成的不同群组。

由图3中 m_1 持有初始密钥 k_{i0} , 可与其他相邻成员组成不同个数的通信组: (m_1, m_2) , (m_1, m_2, m_3) , (m_1, m_2, m_3, m_4) 。

定义2 通信密钥。指通信组内成员之间通信所需的加密密钥。选取通信组中持有最低等级成员的密钥作为通信密钥, 其他高等级的成员都可以根据迭代计算获得通信密钥。如图3中三个通信组的通信密钥分别为: k_{i1}, k_{i2}, k_{i3} , 通信组的其他成员位于较高等级, 都能够通过迭代计算得到通信密钥。由于通信组成员的连续性, 非通信组成员无法计算出此密钥。

3.1.4 框架结构

Level₁: 密钥管理中心 KMC, 负责分配 Level₂ 的密钥集以及成员标识信息, 即主干区域的每个成员 m_i 的映射对 $\langle \text{key ID}, \text{member ID} \rangle$ 以及与之相对应的密钥集 k_{m_i} 。为了保证在分配过程的安全性, KMC 通过离线方式或者在线安全通道的方式将身份标识以及密钥分配给 Level₂ 的每个成员, 并安全保

存在硬件中。

Level₂: OSPF 网络的骨干区域, 每个成员持有来自 Level₁ 预分配的密钥集。Level₂ 包含了所有的 ABR 路由器成员。ABR 不仅是骨干区域的成员, 同时也是其他普通区域的成员, 它替代了 KMC 的工作, 成为 Level₃ 的管理者, 负责分配其所属非骨干区域的普通区域的密钥分配。有的区域可能不只存在一个 ABR, 但只能有一个 ABR 被选举成 Level₃ 的管理者, 记为 AM (Area Manager)。

Level₃: 非骨干区域的普通区域, 此区域的每个成员持有 AM 分配的密钥集, 位于等级结构的最底层。

3.2 密钥分配

3.2.1 分配思想

OSPF 区域可以看成无向图 $G(V, E)$:

$$V = \{v_i | i = (1, 2, \dots, n)\}$$

$$E = \{e_{ij} | i, j = (1, 2, \dots, n), \text{且 } i \neq j\}。$$

顶点 v_i 是区域中的每个合法成员, e_{ij} 表示 v_i 之间的相邻关系, 这种相邻关系也表示了 v_i 之间所具有的哈希迭代关系。

假设图中有 n 个节点 v_i , 每个 v_i 可以看成是一个合法的路由器成员。KMC 共生成 n 条哈希密钥链, 每个 v_i 仅持有每条哈希密钥链的一个密钥。由3.1.3节可知, 不同密钥链的密钥分配与通信组内 v_i 在同一条密钥链中所处的位置有关, 对应图G中则与 v_i 之间的相邻关系有关, 这种相邻关系最终可归结为 v_i 之间的位置排列问题。

任意一个 v_i 与其他成员位置排列的所有情况可以看成 n 个节点的无向完全图。一条汉密顿回路可以表示 v_i 的一种位置排列情况, 那么 n 条无公共边的汉密顿回路就表示 n 种位置排列情况。所以 n 条哈希密钥链密钥的分配方式最多为图中无公共边汉密顿回路的个数。

如果将每个 v_i 排成圆形, 它们的关系只与排序有关。针对于此, 可认为一个成员在圆形中的位置不变, 将其设为1, 并置于圆心, 其他 $n-1$ 个成员的编号排列在圆周上, 则通过圆周的旋转可以得到各边不重复的哈密顿回路。

1) 当 n 为奇数时^[17], 如图4所示。

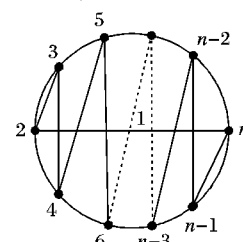


图4 n 为奇数的汉密顿回路图

由图4可以看出, $(1, 2, 3, \dots, n-2, n-1, n, 1)$ 为一条初始汉密顿回路。再将圆周上的节点编号顺时针旋转

$\left(\frac{n-1}{2} - 1\right)$ 次, 且依次旋转 $\frac{2\pi}{n-1}, \frac{2 \times 2\pi}{n-1}, \dots, \frac{\left(\frac{n-3}{2}\right) \times 2\pi}{n-1}$, 分别得到新的汉密顿回路:

$$\begin{aligned} &(1, 4, 2, 6, \dots, n-4, n, n-2, 1) \\ &(1, 6, 4, 8, \dots, n-6, n-2, n-4, 1) \\ &\vdots \\ &(1, n-1, n-3, n, \dots, 2, 5, 3, 1) \end{aligned}$$

所有汉密顿回路构成了一个完全图。

2) 当 n 为偶数时, 将 n 为偶数的情况转化为 $n+1$ 的奇数情况, 寻找 $\left(\frac{n}{2} - 1\right)$ 条汉密顿回路。首先增加一个节点 x , 并认为它的编号大于节点 n 。按照 $n+1$ 为奇数的情况, 除去节点

1,将每一个节点排列在圆周上,得到初始的哈密顿回路(1,2,3,...,n-2,n-1,n,x,1),再将圆周上的节点编号顺时针旋转 $(\frac{n-2}{2}-1)$ 次,且依次旋转 $\frac{2\pi}{n}, \frac{2 \times 2\pi}{n}, \dots, \frac{(\frac{n-2}{2}-1) \times 2\pi}{n}$,但是在旋转过程中,保持节点 x 不作旋转,分别得到新的哈密顿回路:

$$\begin{aligned} & (1,4,2,6,\dots,n,n-3,n-1,x,1) \\ & (1,6,4,8,\dots,n-1,n-5,n-3,x,1) \\ & \vdots \\ & (1,n,n-2,n-1,\dots,5,2,3,x,1) \end{aligned}$$

最后,将找到的哈密顿回路中的节点 x 去除,即可以得到 n 为偶数情况的哈密顿回路。

在 n 为偶数时,实际上只可以得到 $(n-2)/2$ 条无重复哈密顿回路,并不能包含所有的相邻关系。通过添加一个点 x ,补全了遗漏的相邻关系,因此导致了重复的边,但却可以满足构成通信组的条件,进而生成通信密钥达到安全通信的目的。

3.2.2 KMC 密钥分配原理

选取 n 个种子密钥 $sd_i (i=1,2,\dots,n)$,生成 n 条不同的密钥链 $\{k_{i_{j_1}}, k_{i_{j_2}}, \dots, k_{i_{j_r}}, \dots, k_{i_{j_n}}\} (i=1,2,\dots,n; j=1,2,\dots,n)$ 。其中, i 是密钥链的标识,即来自哪一条密钥链; j 是密钥链 i 的第 r 个元素。例如, k_{1_2} 代表密钥链 1 的第 2 个元素所生成的密钥。

已知 n 条哈密顿密钥链标识列表 $\{i_1, i_2, \dots, i_r, \dots, i_n\}$,从每个密钥链抽取一个元素,每个密钥链的初始密钥 k_{i_0} 只能分配给一个成员,作为此成员在一种位置排列下的密钥标识,组成新的密钥链 $\{i_{1_{j_1}}, i_{2_{j_2}}, \dots, i_{r_{j_r}}, \dots, i_{n_{j_n}}\}$ 分配给不同位置排列的每个成员。原理如下:

1) $\{i_1, i_2, \dots, i_r, \dots, i_n\}$ 进行顺序排列,保持顺序不变,下标 $\{j_1, j_2, \dots, j_r, \dots, j_n\}$ 进行 n 次循环置换^[18]。

循环 1:

$$\{i_{1_0}, i_{2_1}, \dots, i_{r_{r-1}}, \dots, i_{n_{n-1}}\} \rightarrow \{i_{1_{n-1}}, i_{2_0}, \dots, i_{r_{r-2}}, \dots, i_{n_{n-2}}\}$$

循环 2:

$$\{i_{1_{n-1}}, i_{2_0}, \dots, i_{r_{r-2}}, \dots, i_{n_{n-2}}\} \rightarrow \{i_{1_{n-2}}, i_{2_{n-1}}, \dots, i_{r_{r-3}}, \dots, i_{n_{n-3}}\}$$

⋮

循环 n :

$$\{i_{1_2}, i_{2_3}, \dots, i_{r_{r+1}}, \dots, i_{n_1}\} \rightarrow \{i_{1_1}, i_{2_2}, \dots, i_{r_r}, \dots, i_{n_0}\}$$

2) 按照 3.2.1 节的思想,将区域中的 n 个成员 m_i 进行编号,排列在圆周上,根据不同的旋转,找到成员的不同位置关系;再将循环置换所得的密钥链依次分配给不同位置排列的成员,如图 5 所示。

a) 当 $n > 4$ 时,若 n 为奇数,则有 $(n-1)/2$ 条哈密顿回路,即对圆周进行 $(n-3)/2$ 次旋转,对成员进行 $(n-3)/2$ 次位置排列,最后将循环置换所得的密钥链依次分配给每一个成员。每个成员应持有 $(n-1)/2 \times n$ 个密钥, $(n-1)/2$ 条密钥链。

b) 当 $n \geq 4$ 时,若 n 为偶数,由于添加一个点,则有 $n/2$ 条哈密顿回路,即对圆周进行 $(n-2)/2$ 次旋转,对成员进行 $(n-2)/2$ 次重排列,最后将循环置换所得的密钥链一次分配给每一个成员。每个成员应持有 $n^2/2$ 个密钥, $n/2$ 条密钥链,分配方法同上。

c) 当 $n < 4$ 时,只有一条哈密顿回路,按照上述方法分配

一次即可。

例如,区域中有 5 个成员 m_1, m_2, m_3, m_4, m_5 ,成员 ID 编号为 1,2,3,4,5。KMC 生成 5 条密钥链,每条密钥链记为 $\{1_0, 1_1, 1_2, 1_3, 1_4\}, \{2_0, 2_1, 2_2, 2_3, 2_4\}, \{3_0, 3_1, 3_2, 3_3, 3_4\}, \{4_0, 4_1, 4_2, 4_3, 4_4\}, \{5_0, 5_1, 5_2, 5_3, 5_4\}$ 。存在 2 条哈密顿回路,即(1,2,3,4,5,1), (1,4,2,5,3,1),如图 6 所示。

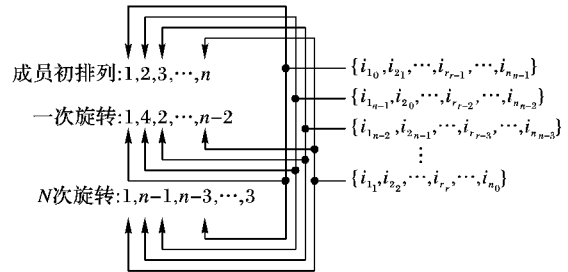


图5 密钥分配图

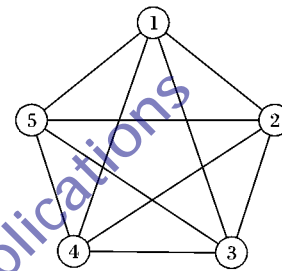


图6 完全图

按照密钥分配原理分配密钥,如表 1 所示,每个成员分配 2 条密钥链,10 个密钥。

表 1 密钥分配表

编号	成员	0 次旋转	1 次旋转
1	m_1	$1_0 2_1 3_2 4_3 5_4$	$1_0 2_1 3_2 4_3 5_4$
2	m_2	$1_4 2_0 3_1 4_2 5_3$	$1_3 2_4 3_0 4_1 5_2$
3	m_3	$1_3 2_4 3_0 4_1 5_2$	$1_1 2_2 3_3 4_4 5_0$
4	m_4	$1_2 2_3 3_4 4_0 5_1$	$1_4 2_0 3_1 4_2 5_3$
5	m_5	$1_1 2_2 3_3 4_4 5_0$	$1_2 2_3 3_4 4_0 5_1$

3.2.3 通信密钥的产生

OSPF 网络中,一个路由器成员产生一条 LSA,将其洪泛到整个网络,就相当于一个成员发送一条信息至多个成员。

发送方和接收方构成了 n 个成员的通信组。如果通信组中的发送成员与任意 $k (1 \leq k \leq n-1)$ 个接收成员属于哈密顿回路的一条连续路径,选取这些成员中编号最小的成员的密钥标识 $k_{i_0}^{(t)}$ (t 代表几次旋转) 的哈希密钥链 i 作为对象,比较分配给 k 个接收成员的来自于同一条哈希密钥链 i 的元素值 j 最大的密钥作为通信密钥。

具体算法如下:

Initialize

give 1 sender and $n-1$ receivers construct a communication group.

Process

- 1) find a continuous path $P_s (1 \leq s \leq g, g \leq n)$ composed by sender and receiver (s) of Hamiltonian cycle t .
- 2) sort P_s by member ID, select key identity $k_{i_0}^{(t)}$ with minimized member ID.
- 3) select $k_{i_{\max(j)}}^{(t)}$.
- 4) $s = s + 1$, if $s > g$, stop. Otherwise go to 1)

3.2.4 AM 密钥分配

Level₂ 骨干区域的成员 m_i 获得 KMC 分配的密钥,将其保存在硬件中。 m_i 作为 Level₃ 子区域的管理者 AM,负责其管

辖子区域的密钥分配工作。

分配原则:将自身所持有的0次旋转密钥链 $\{i_0, i_1, \dots, i_{r-1}, \dots, i_{n-1}\}$ 的元素以第一个元素为基准,两两进行哈希运算^[19],即 $H(i_0, i_1), H(i_0, i_2), \dots, H(i_0, i_{n-1})$,得到新的密钥链的初始值 $i_0', i_2', \dots, i_{n-1}'$ 。由初始值生成 n 条密钥链 $(i_0', i_1', \dots, i_{n-1}')$, $(i_2', i_2', \dots, i_{n-1}')$, \dots , $(i_{n-1}', i_{n-1}', \dots, i_{n-1}')$ 。分配原理同 KMC。

3.3 安全通信

3.3.1 Level₂ 骨干区域成员的通信

Level₂ 骨干区域内的成员 m_i 产生一条LSA,并洪泛到整个区域中。在洪泛之前,成员 m_i 需要:

- 1) 随机选取一个会话密钥 k_s 加密信息数据 $data$;
- 2) 产生通信密钥;
- 3) 使用 k_s 加密信息数据,并对原信息与 k_s 进行哈希运算 $H(k_s + data)$;

4) 将以下信息发布给下一个接收成员 $m_i: (i_{j_1}, i_{j_2}, \dots, i_{j_r})$ 是 m_i 产生的通信密钥的标识列表, i 是哈希密钥链的编号, j 代表属于 i 的第几个元素。 $[E_{k_{i_{j_1}}}^{(i)}(k_s), E_{k_{i_{j_2}}}^{(i)}(k_s), \dots, E_{k_{i_{j_r}}}^{(i)}(k_s)]$ 使用与密钥标识列表相对应的通信密钥加密会话密钥。接收者将接收到的密钥标识与自身所持的 t 值相同的密钥链的元素一一进行对比,如果所持有的密钥标识 i_{j_k} 与接收到的密钥标识 i_{j_r} 位于同一条哈希链 i_r ,并且元素 $j_k \leq j_r$,那么由 $k_{i_{j_k}}^{(i)}$ 经过 $(j_r - j_k)$ 次哈希运算得到 $k_{i_{j_r}}^{(i)}$ 。

通过密钥分配原理所得到的密钥链,总是可以快速产生安全通信密钥,并且只有指定的合法接收成员能够解开密钥,从而获得会话密钥 k_s ,而非法的成员无法获得会话密钥 k_s 。 $E_{k_s}(data)$ 使用了随机选取的会话密钥 k_s 加密数据信息。 $H(k_s + data)$ 使用带密钥的哈希值确保信息在转发过程中没有被修改过,保证源信息的完整性和真实性。

如表1所示:如果成员2产生一条LSA,欲将信息发送至成员3与成员5,将发送如下内容:只有合法的成员3,5,才可以解开会话密钥 k_s ,并获得成员2的网络拓扑信息。成员3,5通过验证 $H(k_s + data)$ 值是否一致来确定成员2洪泛的信息在转发过程中是否遭受修改,是否真实可信,且是否来源于成员2。

3.3.2 Level₃ 子区域成员的通信及与AM之间的通信

Level₃ 子区域成员 sm_i 之间的通信与3.3.1节Level₂区域成员的通信方式原理相同,所不同的是 sm_i 的密钥来自于所属子区域的AM,并不来源于KMC的分配。但是针对Level₃子区域成员 sm_i 与Level₂骨干区域内的成员 m_i 之间的跨层通信,方式是不同的。

AM是子区域的管理者,也是子区域的ABR。每个区域的ABR将其他子区域的信息发布给它所属的子区域内,或者将所属子区域的信息汇总后发布到主干区域中,再转发到其他子区域。AM是子区域密钥的分配者,它可以通过自己的密钥链计算出 n 个哈希密钥链的初始值 $(i_0', i_2', \dots, i_{n-1}')$,利用密钥分配原理分配给 sm_i 。AM可以解开任何 sm_i 的会话密钥 k_s 从而获取数据信息,验证无误后,生成summary LSA发布到其他区域。反过来,它可以利用 $(i_0', i_2', \dots, i_{n-1}')$ 加密会话密钥,再利用 k_s 加密summary LSA的信息数据,发布到子

区域中。即 $\{[i_0', i_2', \dots, i_{n-1}', E_{k_{i_0'}}(k_s), E_{k_{i_2'}}(k_s), \dots, E_{k_{i_{n-1}'}}(k_s)], E_{k_s}(data), H(k_s + data)\}$ 。

4 方案分析

4.1 安全性分析

1) 信息的机密性。

每条信息使用会话密钥 k_s 加密,即 $E(k_s)$,所以信息并不是以明文的形式传输,非通信组内的合法成员不能够获得信息内容,从而保证了信息的机密性。

2) 信息的真实性和完整性。

数据包的尾部附加了会话密钥 k_s 和信息 m 经过哈希运算得到的摘要值,通信组内的合法成员会根据解开的 k_s 和信息内容 m 计算出摘要值进行对比,如果不一致则说明源成员随即选取的 k_s 与信息内容 m 已不再真实可信,如果一致,那么可以确认信息是真实可信的,并且并未遭受篡改。

3) 身份的不可否认性。

KMC和AM预先分配身份标识 $\langle \text{Key ID}, \text{Member ID} \rangle$, $k_{i_0}^{(i)}$ 将会作为Key ID,而Member ID是每个成员的编号。每个成员的身份标识是唯一的,并且Key ID与Member ID是相对应的。只有合法的发送方才如何根据身份标识产生通信密钥,只有通信组指定的合法接收方才能解开密钥。双方都不可以否认其身份。

4) 身份的不可伪造性。

密钥链的生成借助于哈希算法(MD5等),哈希函数的单向性和不可碰撞性使得同区域攻击者很难计算出其他路由器所持有的密钥链。如果想要伪造成某个合法路由器A进行通信,必须要获得它的身份标识和密钥,这对于攻击者是不可能的。

5) 可控性。

密钥保存在路由器的硬件中,通常情况下攻击者是很难获取到的。但是如果子区域的路由器被侵入,并被获取密钥,攻击者不可能通过哈希函数的逆运算获得骨干区域路由器成员的密钥。由此如果威胁一旦发生,可以将其控制在区域内部,而不至于迅速蔓延至全网。如果骨干区域的路由器被强大的攻击者侵入,致使AM不幸沦陷,很可能给子区域的安全带来威胁。针对这点,主动防御手段就不能够起到作用,需要在骨干网络部署相关威胁检测防御系统,对网络进行监控,及时发现网络中的异常情况。

4.2 存储量

如果OSPF网络中有 n 个路由器,那么每个路由器将会产生 n^2 条LSA。OSPF区域的划分可以减少LSA的数量。文献[20]中提出,当每个区域中的路由器都相等时,产生的LSA可以达到最小。假设整个OSPF网的路由器总数为 N (此处不讨论 N 的奇偶性),那么最初应该产生的LSA为 N^2 条;如果将其分为 M 个区域,每个区域应有路由器 N/M ,一共产生的LSA为 N^2/M 条,明显小于未分区域之前。

传统的方案中,每个路由应该存有一个私钥和其他 $N-1$ 个路由器的公钥,一共需要保存 N^2 个密钥。而此方案中,在单个区域内,每个路由器保存 $\frac{N^2}{2M} - \frac{N}{2}$ 个密钥,假设OSPF网络中划分了10个区域,由图7可以看出,随着网络规模的增大,密钥存储量大大降低,且随着划分区域数目的增多,存储量会更大程度地降低。

4.3 系统开销和实时性

1) 与传统方案的比较。

在基于非对称性密码学的传统安全方案中,用于验证数字签名的公钥通过产生一种新的 LSA 的方式洪泛到 OSPF 网络中的每个路由器,称之为 PKLSA。可信第三方预先对 PKLSA 中的证书进行签名,以此证明公钥的可信性。每个 LSA 宣告者优先发送 PKLSA,以保证每个接收者在收到 LSA 之前获取相应的公钥。然而 PKLSA 的发送,有时会出现滞留的情况^[8],使得公钥的处理过程出现一定的时延问题。当路由器接收到 PKLSA 后,使用可信第三方的公钥验证证书,成功后方能得到宣告者的公钥。那么公钥的处理时耗可表示为

$$T_{pk} = \delta + t_{\text{validate}}$$

其中: δ 为 PKLSA 传送过程可能带来的时延, t_{validate} 是可信第三方的公钥验证证书所需的时耗。

OSPF-HS 方案所有的密钥都是预先分配好的,通信密钥可以及时地通过哈希函数的迭代计算得到,其时耗可表示为

$$T_{co} = t_{\text{hash}}$$

很显然,OSPF-HS 方案并没有 PKLSA 的传送时延 δ ,而哈希函数(如 MD5,SHA-1)比数字签名(如 RSA)的速度快很多倍,即 $t_{\text{hash}} \ll t_{\text{validate}}$ 。由此看出, $T_{co} \ll T_{pk}$,新方案大大降低了获取解密密钥的时延,减少了系统开销,从而提高了通信的实时性。

2) 通信密钥生成时耗 T_{co} 分析。

由 3.2.3 节通信密钥生成算法可以看出, T_{co} 与哈希迭代的次数及哈希函数的运算速度有关,而哈希迭代的次数又与通信组的规模有关。在主频为 2.8 GHz 的 Intel Pentium 4 的 PC 上,针对一条 LSA,分别使用不同的哈希函数算法 MD5、SHA1、SHA256、SHA384 和 SHA512 进行实验,图 8 描述了随着通信组规模变化时 T_{co} 的变化趋势。

哈希函数算法 SHA 系列与 MD5 相比,运算速度相对较慢,产生通信密钥的时耗更大。所以从系统开销和实时性方面来说,MD5 更占优势。

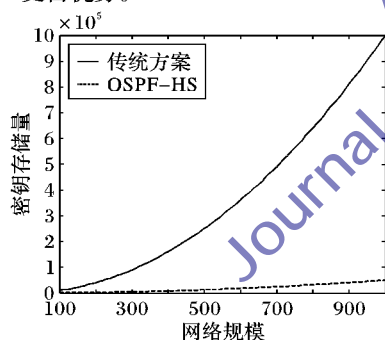


图7 存储量对比

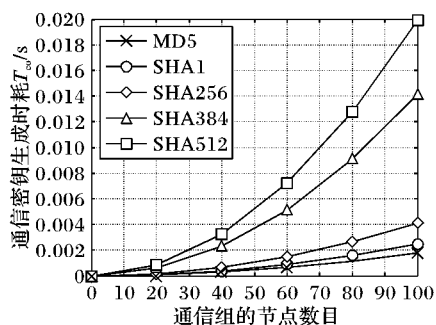


图8 通信密钥生成的时耗 T_{co}

5 结语

OSPF 网络的安全性问题一直是网络安全领域的关注重点。针对主动防御策略,基于密码学的解决方案一直是最为可取的。然而就目前来说,传统方案大多从非对称性密码算法的解决方案——数字签名考虑,一直存在着存储量大、系统

开销大以及通信实时性不强等问题,同时密钥分配与管理方案也不适用于 OSPF 网络原有的二层等级结构。本文就以上问题提出了新的方案,详细阐述了方案实现的原理,并就安全性、存储量及实时性进行了分析。分析表明本文方案不仅适用于 OSPF 的二层等级结构,实现了端到端、点到点的安全认证,保证了源数据的可信性和真实性,而且降低了存储量和系统开销,提高了实时性和稳定性。

参考文献:

- [1] REKHER Y, LI T, HARES S. RFC 4271, A border gateway protocol 4 (BGP-4) [S]. Reston: IETF, 2006.
- [2] MALKIN G. RFC 2453, RIP Version 2 [S]. Reston: IETF, 1998.
- [3] MOY J. RFC 2328, OSPF version 2 [S]. Reston: IETF, 1998.
- [4] ORAN D. RFC 1142, OSI IS-IS intra-domain routing protocol [S]. Reston: IETF, 1990.
- [5] JONES E, LE MOIGNE O. OSPF security vulnerabilities analysis [EB/OL]. (2006-06-16) [2012-12-09]. <http://tools.ietf.org/html/draft-ietf-rpsec-ospf-vuln-02>.
- [6] HARTMAN S, ZHANG D. RFC 6863, Analysis of OSPF security according to the keying and authentication for routing protocol (KARP) Design Guide[S]. Reston: IETF, 2013.
- [7] BHATIA M, MANRAL V, FANTO M, et al. RFC 5709, OSPF HMAC-SHA cryptographic authentication [S]. Reston: IETF, 2009.
- [8] MURPHY S, BADGER M, WELLINGTON B. RFC 2154, OSPF with digital signatures [S]. Reston: IETF, 1997.
- [9] 李道丰, 杨义先, 谷利泽, 孙斌. 采用可净化签名的 OSPF 协议安全保护机制[J]. 北京邮电大学学报, 2011, 34(3): 79-83.
- [10] DECCIO C T, CLEMENT M, SEAMONS K. Securing OSPF using digital signatures and neighbor checking [EB/OL]. [2012-11-26]. <http://dna.cs.byu.edu/papers/pdf/ospf.pdf>.
- [11] BRUHADESHWAR B, KOTHAPALLI K, POORNIMA M, et al. Routing protocol security using symmetric key based techniques [C]//ARES '09: Proceedings of the Fourth International Conference on Availability, Reliability and Security. Washington, DC: IEEE Computer Society, 2009: 193-200.
- [12] YU M. Security enhancements to routing protocols for backbone networks [C]// SMC '06: Proceedings of the 2006 IEEE International Conference on Systems, Man, and Cybernetics. Piscataway: IEEE, 2006, 3: 1891-1896.
- [13] THOMAS T. OSPF network design solution [M]. 2nd ed. Indianapolis: Cisco Press, 2003.
- [14] 秦科, 张小松, 郝玉洁, 等. 网络安全协议 [M]. 成都: 电子科技大学出版社, 2008.
- [15] 施荣才, 翁丽萍, 王国才. 基于单向哈希链的 Ad Hoc 网络密钥协商协议[J]. 湖南大学学报: 自然科学版, 2010, 38(3): 77-81.
- [16] HUANG D, MEDHI D. A key-chain based keying scheme for many-to-many secure group communication [J]. ACM Transactions on Information and System Security, 2004, 7(4): 523-552.
- [17] 北京交通大学, 计算机与信息学院. 在无向完全图中寻找边不重复的汉密尔顿回路[EB/OL]. (2005-06-07) [2012-12-16]. <http://www.doc88.com/p-402265120707.html>.
- [18] 许春香, 周俊辉. 信息安全数学基础 [M]. 成都: 电子科技大学出版社, 2008.
- [19] HUANG D, MEDHI D. A secure group key management scheme for hierarchical mobile Ad Hoc networks [J]. Ad Hoc Networks, 2008, 6(4): 560-577.
- [20] AHO A V, LEE D, HILL M. Hierarchical networks and the LSA N-squared problem in OSPF routing [C]// GLOBECOM '00: Proceedings of the 2000 IEEE Global Telecommunications Conference. Piscataway: IEEE, 2000, 1: 397-404.