计算机科学 2005Vol. 32№. 11

一种安全的移动自组网链路状态路由协议:SOLSR

洪 帆 洪 亮 付 才

(华中科技大学计算机科学与技术系 武汉 430074)

摘 要 移动自组网是一种新型的无线移动网络,具有无中心、自组织、拓扑结构变化频繁以及开放式通讯信道等特性,因此移动自组网下的路由协议所面临的安全问题比有线网环境下更为严重。OLSR(Optimized Link State Routing)协议于2003年成为RFC3626草案[1],该协议首先假设网络中所有节点都是友好的,无恶意行为,同时认为安全问题可以利用IPSec来解决,但是,OLSR协议的通讯通常是"一对多"的广播形式,IPSec是针对端到端通讯的安全方案,故而单单依靠IPSec并不能完全解决OLSR的安全问题。由于OLSR自身还存在着机制上的漏洞,恶意节点针对这些漏洞进行攻击,可以导致路由协议无法正常工作,继而影响到整个网络的运行。本文在对OLSR的安全性分析的基础上,对协议进行了改进,加强了协议中对"邻居关系"的定义,同时引入了虫洞检测和身份认证机制,以及通讯报文的安全附加项,从而提出了安全链路状态路由协议——SOLSR来保证移动自组网中路由协议的正常运行。

关键词 移动自组网,安全路由,虫洞检测,散列链表

SOLSR: A Secure Link State Routing Protocol for Ad Hoc Networks

HONG Fan HONG Liang FU Cai

(Department of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074)

Abstract Mobile Ad hoc Netwoks(MANET)is a new networking paradigm for wireless hosts. Because of self-organization, dynamic topology and openness of wireless links, the routing security in MANET is more seriously than in wired networks. Optimized Link State Routing(OLSR)is proposed by IETF's MANET Group at 2003. OLSR assumes that all nodes in the netwoks are all friendly, and if there exist some security problems , IPSes can solve it . But OLSR's packets are often broadcasted and IPsec provides end-to-end security, so relying on IPSec isn't enough. Due to some existing defects, OLSR may not work if malicious nodes attack against routing. In this paper, we first analyze the OLSR's security, then propose a solution to secure OLSR— SOLSR, which strengthenes the neighbor relationship establishment, applies the worm-detective mechanism and authentication, and protects routing information.

Keywords Mobile ad hoc network, Secure routing, Worm-hole attack detective, Hash chain

1 引言

移动自组网是一种临时自治的分布式系统,具有无中心、自组织、网络拓扑结构变化频繁等特征。作为支撑网络的基础构件之一的路由协议便受到越来越多的学者和研究团队的关注。移动自组网的路由协议大体分为两类:表驱动的预先型路由和源起始的按需型路由。IETF专门成立了MANET工作组来研究移动自组网的路由方案,其中DSR(dynamic source routing)[2]和AODV(ad-hoc on demand distance vector routing)[3]是按需型路由协议,只有在需要和对方通讯的时候,才开始查找路由;OLSR是基于链路状态的移动自组网路由协议,属于表驱动型路由协议。

由于没有固定的网络基础设施、网络拓扑结构频繁动态变化、无线信道完全开放、网络缺乏自稳定性等原因,移动自组网环境下的路由协议相对于有线网环境下的更易遭受各种攻击,比如路由报文的篡改、假冒节点进行路由行为、黑洞攻击、拒绝服务以及虫洞攻击(Wormhole attack)等等,因此设计安全的路由协议非常重要。

OLSR协议(RFC3626)假设移动自组网络中的节点都是友好的,同时认为涉及安全的问题可以利用IPSec来解决。IPSec在解决点到点的安全通讯方面(即单播的情况下)是有优势的,但对于广播或者组播的情况,就不太适合,而在OLSR的路由查找和发现的过程中,路由包以广播或者组播的形式比较常见,所以单单依靠IPSec来解决移动自组网的安全问题是不够的。本文将主要针对OLSR协议进行安全性分析,在分析的基础上提出一种适合OLSR的安全路由协议——SOLSR。

康乃尔大学的Zhou和Haas在文[4]中详细描述了移动自组网所面临的安全问题,尤其强调了"安全路由"的问题,同时认为"针对路由协议发动的拒绝服务攻击"将对网络造成毁灭性的后果,指出了"一个安全的路由协议对于移动自组网的重要性"。

关于移动自组网中安全路由协议的设计,国外很多家研究机构已经提出自己的方案,比较有名的如下。

Papadimitratos和Haas提出的SRP[5]安全协议框架,可以应用于现存的几种协议(主要适用于DSR)。SRP假设在通信的两个节点间存在一个安全关联SA(Security Association),通过SA进行双向验证来保证两个通信节点间路由信

洪 帆 教授,博士生导师,主要研究领域为计算机安全与保密,长期从事信息安全理论和技术的研究与开发。洪 亮 博士研究生,主要研究领域为无线局域网环境中的安全问题。付 才 博士研究生,主要研究领域为网络安全。

息的准确性，这样在路由请求过程中就可以不考虑中间节点的安全性。但 SRP 协议并没有提供路由差错报文的安全保护，因而恶意节点可以伪造差错报文来攻击源节点。

Dahill 等提出的 ARAN[6] 路由协议，在协议中需要身份认证，因而一个可信赖的认证服务器 CA 是必须的。在 ARAN 中，每个节点中转一个路由包或者回复一个路由请求包，都需要对包签名，这将导致节点的开销过大，而且包的长度每经过一个节点都将增加。除此之外，如果节点没有时钟同步，易遭受重放攻击。

文[7]中提出了一种基于 DSR 和 TESLA 的安全按需路由协议——Ariadne，Ariadne 分为三个阶段：1）提出一种允许目的节点验证路由请求的机制。2）提出了三种可以互换的机制来验证路由请求和路由回复中的数据。3）提出了一种有效的哈希算法来验证路径上的每个节点都不能缺少。但该协议要求网络中所有节点的时钟严格同步，这一点在移动自组网实现起来比较困难。

SEAD[8] 是 Hu，Johnson 和 Perrig 提出的一种基于距离矢量路由协议 DSDV 安全路由协议。通过让哈希值和路由信息中的权值以及序列号相关联，使用单向哈希函数来防止恶意节点减小路由信息中对应目的节点的权值或者增加它的序列号。

本文第 2 节对 OLSR 协议作一个概述性的描述，同时对其进行安全性的分析，指出其不足和需要改进的地方；第 3 节是在上一节的基础上，提出适合 OLSR 的安全方案 SOLSR；第 4 节，对 SOLSR 进行分析，并对其中关键机制进行形式化分析和证明；最后是全文的总结。

2 OLSR 简介及其安全需求

2.1 协议简介

OLSR 协议(Option Link State Routing)是一个表驱动预设型路由协议，网络中的节点周期性地与其它节点交换拓扑消息。每个节点选择某些邻居节点作为其“多点中继(MPR)”(本文简称为中继代理)，只有被选为中继代理的节点负责转发该节点的拓扑消息(Topology Control Message)。OLSR 协议通过引入中继代理的机制来减少所需转发的消息数量，从而提供了一种控制消息洪泛的有效机制，因而非常适用于大型密集的移动网络，网络规模越大节点越密集，与传统的链路状态算法相比就越能取得最优。

在移动自组网中，每一个节点都保持了一个中继代理表(MPR Table)和中继雇主表(MPR Selector Table)，中继代理表保存的是被节点 A 从邻居集合中选择出来，负责转发 A 的拓扑控制消息的邻居节点，即 A 相对于中继代理表中的每个节点而言，是中继雇主。而中继雇主表保存的是所有选择 A 作为中继代理人的节点，即 A 相对于中继雇主表中的每个节点而言，则是中继代理人。

OLSR 协议包含四个重要的过程：邻居探测、中继代理选择、路由控制消息的发布、路由表计算等过程。其中中继代理选择和路由表计算都是在节点的终端上处理的过程，这里主要说明一下邻居探测和拓扑控制消息发布的过程。

OLSR 的邻居探测是通过定期广播邻居探测消息(间隔时间是 2s)来实现的，邻居探测消息包含有发布节点 A 的信息以及它的邻居信息。A 的邻居，比如节点 B，接收到 A 的探测包后，先检测其邻居表中是否有 A，若没有，则将 A 添加到邻居表中；若已存在，则刷新 A 的存活时间。当在一个固定的时间间隔内没有接收到来自 A 的探测包时，B 将把 A 从邻居表中删除。要注意的是，邻居探测消息只对其邻居广播，邻居接收到报文后，但不转发报文，对于“不转发报文”这点，OLSR 协议没有强制性措施（转发报文会引发某种攻击，这一点将在后文中详述）。

在邻居表更新，进行中继代理选择之后，每个节点将定期广播拓扑控制消息，拓扑控制消息中包含发布节点的邻居信息，拓扑控制消息是通过节点的中继代理来广播到全网络中去，其它节点收到消息后，根据消息的序列号来决定是否接收该消息。

2.2 OLSR 存在的漏洞

OLSR 协议没有充分考虑移动自组网环境的恶劣性和潜在的不安全性，其假设的前提——网络中所有节点都是友好的——并不恰当。由于 OLSR 中所有的信息报文都是以广播形式传输的，若想通过引入 IPSec 来解决其安全问题，并不合适宜，因为 IPSec 提供的是一个端到端的安全信道，而 OLSR 的信息传输是一对多的，所以设计一个 OLSR 的安全方案必须考虑到这一特点。针对 OLSR 的特点，恶意节点可以通过以下途径来发动攻击：

1. 由于没有身份认证过程，恶意节点成为某个节点的邻居之后，就有可能成为该节点的中继代理，成为中继代理之后，就可以对该节点的拓扑信息，进行不转发，或者有选择性的转发，或者窜改，或者重放等等攻击行为，导致其他节点无法获得该节点的正确信息，从而干扰拓扑图的形成；

2. 由于 OLSR 协议没有提供一个源鉴别机制，因此恶意节点可以像正常节点一样发布拓扑信息，不过其发布的都是一些虚假错误的信息，其他节点无法辨别真假，从而干扰了拓扑图的形成；

3. 由于网络上传输的路由报文都是明文而且没有安全性的保护措施，因而恶意节点可以随意修改报文的内容，形成攻击。

4. 在节点进行邻居探测过程中，恶意节点在距其一跳的距离内接收该报文后，通过某种方式(比如虫洞形式)，将其转发到另外一个区域，导致本不在一跳距离的两个节点形成邻居节点。

这里重点描述一下第 4 种攻击。为了叙述方便，约定以下符号：A－＞ ＊：content，表示 A 广播内容为 content 的报文；A－＞ B：content，表示 A 向 B 发内容为 content 的数据包。

在图 1 中，A 和 B 是两个合法节点，但彼此不在对方信号覆盖范围内，M 为恶意节点，同时在 A 和 B 的信号覆盖范围内，如图 1 所示。其中圆圈代表节点的信号覆盖范围。

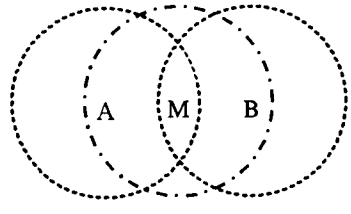

图 1 节点分布示意图

攻击过程如下：

1. A－＞＊：A，NS，Neighbor(A)，其中 NS(Neighbor Sensing)表示报文类型是邻居探测类型，Neighbor(A)表示节点 A 的邻居集合；

2. M—>*：A，NS，Neighbor(A)；

3. B将把A添加到邻居集合Neighbor(B)中去；

4. B—>*：B，NS，Neighbor(B)，其中Neighbor(B)表示节点B的邻居集合；

5. M—>*：B，NS，Neighbor(B)；

6. A将把B添加到邻居集合Neighbor(A)中去。

这样，恶意节点M便导致A和B互相认为对方是自己的邻居，然后两节点将把这一错误信息通过拓扑信息报文散播到全网络中去，导致节点在形成路由表时出现错误。

为了解决这一问题时，可以借鉴文[9]中的"看门狗"机制，节点广播邻居探测包之后，同时将这个包拷贝到一个缓冲区里，然后监听网络，若在一个探测周期内，发现监听到同样的报文，就知道某个恶意节点潜伏在自己信号覆盖范围内转发了邻居探测包。基于这个思想，当M在转发A的邻居探测包时，由于线路是开放的，因此A同样能收到该报文，A将此报文与缓冲区内缓存的对象进行比对，发现一致，便可探测到这种攻击行为。不过这一机制当遇到有两个以上的恶意节点联合发动"虫洞攻击"[10]时，就无效了。如图2所示。

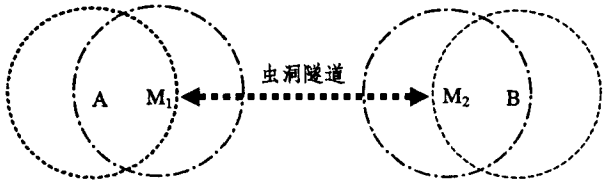

图2 虫洞攻击示意图

其中，M_1和M_2是两个恶意节点，它们可以通讯，通讯的内容将用会话密钥加密。攻击如下：

1. A—>*：A，NS，Neighbor(A)；

2. M_1—>M_2：$\{A, NS, Neighbor(A)\}_K$，其中报文用M_1和M_2的密钥K加密，因而中间节点无法得知报文内容；

3. M_2—>*：A，NS，Neighbor(A)；

4. B将把A添加到邻居集合Neighbor(B)中去；

5. B—>*：B，NS，Neighbor(B)；

6. M_2—>M_1：$\{B, NS, Neighbor(B)\}_K$；

7. M_1—>*：B，NS，Neighbor(B)；

8. A将把B添加到邻居集合Neighbor(A)中去。

因为M_1和M_2接收到探测包后，并没有广播，而是以加密后的普通数据包形式发给虫洞的另一端，由另一端解密后再广播，从而A(或者B)无法探测到这种攻击，进而导致双方互相认为对方是自己的邻居。虫洞攻击中，攻击者无须知道合法节点的机密信息，只是简单地接收和转发报文，便可导致节点在形成自己的邻居集合时出错，当节点向全网其他节点广播自己的链路状态(即拓扑消息)后，错误将扩大至全网，使每个节点形成有错误的网络拓扑图，形成的路由表将是不可用的。

综上所述，OLSR协议的安全需求如下：

1. 在邻居探测过程中，应能提供一个检测虫洞攻击的机制；

2. 在确定邻居关系过程中，应该有一个身份认证的机制，以确保邻居是合法节点，从而保证中继代理选择过程中不会有恶意节点成为中继代理；

3. 应对网络上传输的信息报文提供一个安全机制，以防御窜改、重放等等恶意行为；

4. 应对广播的报文提供一个源鉴别机制，使得接收节点可以验证所接收的报文是否为合法节点所广播。

3 SOLSR—基于OLSR的安全路由协议方案

3.1 概述

为了解决上述问题，我们提出了基于OLSR的安全协议方案——SOLSR，它将从两个方面加强OLSR的安全性，其一，邻居探测的安全机制加强，只有在信号覆盖范围内，并通过了身份验证的，才能被确认为邻居；其二，协议报文的安全性加强，由于OLSR中只有广播报文，因此应该提供一个这样的机制，即接收者可以验证发布者的身份，同时可以验证报文完整性的机制。至于抗重放攻击，由于OLSR协议中已经确定每个节点所发的报文都具有一个唯一的序列号，只要在完整性保护中保护序列号不被窜改，就可以抗报文重放攻击。

下面将具体阐述方案。

3.2 前提假设

方案将假设网络中节点之间的通讯是双向的，即若节点A可以接收到来自B的数据包，则B一定可以接收到来自A的数据包。同时每一个合法节点具有公私钥对(K_i/K_i^{-1})，以及由可信的第三方发布的公钥证书$(Cert_i)$，网络中应存在一个这样的可信第三方负责为合法节点产生、更新、撤销公钥证书，而且节点可以验证其他节点所提供证书的合法性。这里要强调的是，只有合法节点才可以获得可信第三方的公钥证书，也只有合法节点之间才能互相信任，互相通讯，至于合法节点的拜占庭行为，可以利用文[11]中提出的可信度模型进行探测和预防，在本文中暂不讨论。

公钥证书的格式如下：

$Cert_i=\langle ID, K_i, VTime_i\rangle_{K^{-1}}$，ID是节点$i$的在网络中的唯一标识，$K_i$是它的公钥，VTime是这个证书的有效期，$K^{-1}$是可信第三方的私钥。

3.3 邻节点安全探测机制

由OLSR协议的安全性分析可知，针对邻居探测过程的虫洞攻击，可以对网络的运行造成毁灭性的攻击。因而在SOLSR协议中，如何防御和检测虫洞攻击将是保证路由协议能正常运行的首要条件。

虫洞攻击的特点是，"攻击者在隧道的一端将邻居探测报文接收，然后在另一端重放，用隧道将两端的实际距离压缩成一跳距离"[10]，从而达到邻居欺骗的目的。这个攻击利用了原协议中对邻居定义的不完整性，即只要节点收到某个探测报文便可认定发布者在自己的信号覆盖范围内，从而认定发布者就是自己的邻居。

SOLSR协议对邻居的定义如下：

只有互相在对方信号覆盖范围内(即一跳距离内)，且通过身份验证的才可以互相确定为邻居。

第一句话就是要保证当一个节点收到某个探测报文时，还要确定这个报文只广播了一跳距离。第二句话是要保证在信号覆盖范围的这个节点是合法节点，以确保在中继代理选择过程中，选择出来的代理人都是可信的节点。

SOLSR协议的邻居安全探测机制便是保证第一点的。由于虫洞攻击中，广播报文从一端接收，在另一端重放，中间的实际传输距离肯定大于一跳距离。如果能计算出一端接收到另一端释放之间的时间差t，便可以计算出隧道的长度s(即报文实际传输距离)，即$s=t\times c$(假设数据包的发送和接收时间可以忽略不计)，其中c是无线信号的传播速度，通常

等于光的速度。同时节点的信号覆盖范围的半径是和其自身的无线装备有关，通常这个值 r 是一个定值(例如，如今市面上的流行的无限网卡，其信号覆盖半径大约是 200 米～300 米)。那么由计算得出的 s 和 r 相比，若 $s>r$，就表明隧道存在，节点所收到的邻居探测报文是经过转发的，于是检测出虫洞攻击；反之，就表明节点收到的确实是广播了一跳距离的报文。

在 SOLSR 协议中，当节点 B 收到节点 A 的探测报文时，且 A 不在 B 的邻居集合中，将执行以下步骤：

· B 先发给 A 一个试探数据包，同时产生一个计时器，开始计时；

· 当 A 收到 B 的试探包后，立即对 B 回应，同时也产生一个计时器，开始计时；

· B 收到回应后，停止计时，记下这个间隔时间 $\triangle t_b$，同时对 A 的回应再产生一个回应，之后计算 B 与 A 的距离 $s=(\triangle t_b/2)\times c$，若 $s>r$，则认为 A 不是自己的邻居，退出，反之，则与 A 进行身份认证过程；

· A 收到 B 的回应后，不用再产生回应，其他的处理过程如 B 一样。

这个机制相比文[7]中的检测机制有个好处，即不要求网络中所有节点必须时钟同步，因为时间间隔是由节点自己的时钟计时得到的。

通过上述检测正常之后，节点之间将进行身份认证过程。

1. A 产生一个大的随机数 R_A(其位数和安全级别有关)，然后将公钥证书和节点标识填充到报文中，报文最后附加上 A 对报文的散列值的签名，发送给 B。公式中的 H 为单向散列函数：

$A\rightarrow B: A, B, Cert_A, R_A, sign(H(A, B, Cert_A, R_A))$

2. B 收到 A 的报文后，先验证 A 的公钥证书，然后用公钥证书中所包含的 A 的公钥验证签名，有效之后，产生一个大的随机数 R_B，将其和自己的公钥证书以及节点标识填充到报文，然后附加上 B 对上述项进行单向散列运算之后的签名，发送给 A：

$B\rightarrow A: B, A, Cert_B, R_B, sign(H(B, A, Cert_B, R_A, R_B))$

3. A 先验证 B 的证书，若证书有效，然后验证签名，签名也有效的话，A 便可确定 B 是自己的邻居，同时 A 将产生对 B 的回应报文：

$A\rightarrow B: A, B, sign(H(A, B, R_A, R_B))$

4. B 收到 A 的报文，验证签名有效后，就可以确定 A 是自己的邻居。

经过上述两个步骤，节点 A 和 B 便可以确认双方是邻居关系。邻居安全探测机制的结构图如图 3 所示。

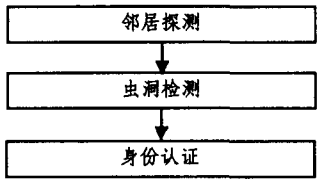

图 3　邻居安全探测机制结构图

3.4　协议报文的安全附加项

在 OLSR 协议中，所有的消息都是广播形式的，为了抵抗恶意节点广播虚假消息、窜改正常节点的报文等等，SOLSR 应提供一个报文的完整性校验以及接收者验证发布者的机制。

OLSR 的消息格式如下：

Message Type	Vtime	Message Size
Originator ID		
Time To Live	Hop Count	Message Sequence Number
MESSAGE		

图 4　OLSR 的消息格式

由图 4 可知，OLSR 的消息项分为两类，一种是在传输过程中不变的，一种是在传输过程中要改变的，例如 Time To Live 和 Hop Count 项。针对内容不变的，可以利用数字签名来保证其完整性。对于内容可变项——Time To Live 和 Hop Count，其二者是为了限制报文可传递的范围，可以利用单向散列链表来保证被正确的递减。当发布者要发布消息时，先产生一个随机数 Seed，然后对 Seed 进行 Time To Live 次单向散列运算，其值 $Hash\_Hop=H^{Time\ To\ Live}(Seed)$。安全附加项的格式如下。

Type	Reserved
Hash_Hop	
Seed	
Signature	

图 5　SOLSR 安全报文扩展项

当节点接收到其他节点发布的消息时，决定是否继续转发时，将执行以下步骤：

· 先计算 $h^{Time\ To\ Live-Hop\ Count}(Seed)$ 是否和 Hash_Hop 的值相等，若不相等，则表明 Hop Count 被改动过，退出；反之，进行下一步；

· 对 Time To Live 自减 1，若大于 0，表明要继续广播该报文，对 Hop Count 自加 1，同时 Seed=h(seed)，然后转发报文。

图 5 中的 Signature 是发布者对消息中所有不变项进行散列运算后的数字签名。

至此，SOLSR 的报文由于有了安全附加项，保证了报文的完整性，也保证了报文接收者可以验证发布者是否合法为合法节点。

4　SOLSR 协议的分析

SOLSR 协议安全性的基础在于这一假设前提“合法节点才能拥有有效的公钥证书”。由于恶意节点没有合法的公钥证书，因而其发布的虚假拓扑消息没有有效的数字签名，其他节点将拒绝接收；由于没有合法的公钥证书，恶意节点无法在身份认证过程中提供有效的凭据，因此成为不了合法节点的邻居，也就不可能成为合法节点的中继代理；至于针对网络上传输的路由报文进行窜改、重放等等攻击行为，由于 SOLSR 的协议报文有完整性校验和抗重放机制，因此也不能得逞；针对邻居探测过程的虫洞攻击，利用虫洞检测机制，检测出报文实际的传输时间，然后计算出报文的传输距离，即节点之间的实际距离，便可检测出是否有虫洞攻击发生。

网络的密钥管理部分可采用两种方式，一种是分散的 CA 形式，一种是自组织的形式。文[4]中提出了一种基于 Shamir 门限方法的分布式密钥认证体系。它将 CA 的私钥分

解成N个部分，每个部分由一个节点存储。其中任意K个节点可以恢复出这个私钥，从而充当CA，完成证书的签发工作。文[12]提出了一种基于多跳步加密签名函数签名的安全分布式认证方案，即将移动密码学与门限加密分布式认证相结合，并采用了分布式容错处理算法和私钥分量刷新技术。文[13]中提出了一种类似于PGP的自组织密钥系统，系统通过证书链来实现CA的功能。一个节点存储它所信任的节点的证书。如果一个节点想获得另一个节点的证书，那么它就顺着证书链去查找，直到找到为止。

由于身份认证过程是SOLSR协议的关键过程，这里利用BAN逻辑[14]，并采用文[15]中的符号和推理规则，对SOLSR协议中的身份认证过程进行形式化分析，论证其正确性。附录中有具体的符号说明。

身份认证过程中的三条消息可以形式化表示为以下三条语句，其中A和B是认证的两个实体，K_s^{-1}是认证机构S的私钥：

1. $A\rightarrow B:\{\xrightarrow{k_a}A\}_{k_s^{-1}},R_b,\{H(\xrightarrow{k_a}A,R_a)\}_{k_a^{-1}}$

2. $B\rightarrow A:\{\xrightarrow{k_b}B\}_{k_s^{-1}},R_b,\{H(\{\xrightarrow{k_b}B,R_a,R_b)\}_{k_b^{-1}}$

3. $A\rightarrow b:\{R_a,R_b\}_{k_a^{-1}}$；

身份认证的目的是要A相信消息2中的签名确实来自于B，B相信消息1和3的签名确实来自于A，换言之，要证明A相信B拥有私钥k_b^{-1}，B相信A拥有私钥k_a^{-1}，即$A|\equiv B\ni k_b^{-1}$和$B|\equiv A\ni k_a^{-1}$。

初始假设为如下：

(i)$A|\equiv\xrightarrow{k_a}A,A|\equiv\xrightarrow{k_s}S,A\ni k_s,A|\equiv S\Rightarrow\xrightarrow{k_b}B,A|\equiv\#(R_a),A|\equiv\#(\{\xrightarrow{k_b}B\}_{k_s^{-1}}),A|\equiv\phi(\{\xrightarrow{k_b}B\}_{k_s^{-1}})$

$B|\equiv\xrightarrow{k_b}B,B|\equiv\xrightarrow{k_s}S,B\ni k_s,B|\equiv S\Rightarrow\xrightarrow{k_a}A,B|\equiv\#(R_b),B|\equiv\#(\{\xrightarrow{k_a}A\}_{k_s^{-1}}),B|\equiv\phi(\{\xrightarrow{k_a}A\}_{k_s^{-1}})$

显然，A确信k_a是自己的公钥，k_s是认证机构S的公钥，同时相信S对k_b是否是B的公钥的判断；A可以产生有效的随机数R_a，A相信B的公钥证书的时间有效性；由于公钥证书的格式是公认的，自然B的公钥证书是可以认知的。类似地，关于B的假设条件如第二行：

(ii)由认知规则可得$\dfrac{B|\equiv\phi(\{\xrightarrow{k_a}A\}_{k_s^{-1}}),B\ni k_s}{B|\equiv\phi(\xrightarrow{k_a}A)}$；

由消息1有$\dfrac{B\lhd\{\xrightarrow{k_a}A\}_{k_s^{-1}},B\ni k_s,B|\equiv\phi(\xrightarrow{k_a}A)}{B|\equiv S|\sim\{\xrightarrow{k_a}A\}}$，$B$见过$A$的公钥证书，$B$拥有$S$的公钥，而且公钥证书是可以认知的，自然就可以推出$B$确信$S$曾发布过$A$的证书；

由时间有效法则可知$\dfrac{B|\equiv\#(\{\xrightarrow{k_a}A\}_{k_s^{-1}}),B\ni k_s}{B|\equiv\#(\xrightarrow{k_a}A)}$；

由前两式，B可推出S相信k_a是A的公钥这一事实，

$\dfrac{B|\equiv S|\sim\{\xrightarrow{k_a}A\},B|\equiv\#(\xrightarrow{k_a}A)}{B|\equiv S|\equiv\xrightarrow{k_a}A}$；

由权限法则得到$\dfrac{B|\equiv S|\Rightarrow\xrightarrow{k_a}A,B|\equiv S|\equiv\xrightarrow{k_a}A}{B|\equiv\xrightarrow{k_a}A}$，即$B$相信$k_a$是$A$的公钥；

(iii)由消息2，类似(ii)可先得到：

$\dfrac{A|\equiv\phi(\{\xrightarrow{k_b}B\}_{k_s^{-1}}),A\ni k_s}{A|\equiv\phi(\xrightarrow{k_b}B)}$，

$\dfrac{A\lhd\{\xrightarrow{k_b}B\}_{k_s^{-1}},A\ni k_s,A|\equiv\phi(\xrightarrow{k_b}B)}{A|\equiv S|\sim(\xrightarrow{k_b}B\}}$，

$\dfrac{A|\equiv\#(\{\xrightarrow{k_b}B\}_{k_s^{-1}}),A\ni k_s}{A|\equiv\#(\xrightarrow{k_b}B\}}$，

$\dfrac{A|\equiv S|\sim\{\xrightarrow{k_b}B\},A|\equiv\#(\xrightarrow{k_b}B)}{A|\equiv S|\equiv\xrightarrow{k_a}B}$，

$\dfrac{A|\equiv S|\Rightarrow\xrightarrow{k_b}B,A|\equiv S|\equiv\xrightarrow{k_b}B}{A|\equiv\xrightarrow{k_b}B}$，即$A$相信$k_b$是$B$的公钥；

又因为$\dfrac{A|\equiv\#(R_a)}{A|\equiv\#(\xrightarrow{k_b}B,R_a,R_b)}$，$\dfrac{A|\equiv\#(\xrightarrow{k_b}B,R_a,R_b)}{A|\equiv\#(H(\xrightarrow{k_b}B,R_a,R_b))}$，

由以上结论便可以得到下面式子：

$$\frac{A\ni\{H(\xrightarrow{k_b}B,R_a,R_b)\}_{k_b^{-1}},A\ni k_b,A|\equiv\xrightarrow{k_b}B,A|\equiv\phi(H(\xrightarrow{k_b}B,R_a,R_b)),A|\equiv\#(H(\xrightarrow{k_b}B,R_a,R_b))}{A|\equiv B\ni k_b^{-1}}$$

即A相信B拥有k_b^{-1}，则B的身份得到证明；

(iv)由消息3以及(ii)中的结论，可得到下列结论，

$$\frac{B\ni\{H(R_a,R_b)\}_{k_a^{-1}},B\ni k_a,B|\equiv\xrightarrow{k_a}A,B|\equiv\phi(H(R_a,R_b)),B|\equiv\#(H(R_a,R_b))}{B|\equiv A\ni k_a^{-1}}$$

，即B相信A拥有k_a^{-1}，A的身份得到证明。

经过对三条消息的形式化分析和证明，可知身份认证的目的达到，即$A|\equiv B\ni k_b^{-1}$和$B|\equiv A\ni k_a^{-1}$。

结论 通过对RFC3626—OLSR协议进行分析之后，指出了单单依靠IPSEC来保证协议的运行的想法是不可行的。本文所提出的SOLSR协议，采用了邻居安全探测机制，减小了虫洞攻击的可能性；引入身份验证过程之后，加强了邻居关系确定的条件，确保了节点在中继代理选择时，不会出现恶意节点被选中的情况；安全附加项利用数字签名和单向散列链表，为网络上传输的协议报文提供了安全机制，满足了完整性校验和源鉴别的安全需求。

附录

本文用到文[13,14]中的基本符号如下，其中X和Y表示任意语句，P和Q表示主体，K和K^{-1}分别表示公钥和私钥。

- (X,Y)：表示两个语句的连接。
- $H(X)$：表示对X进行单向散列运算。
- $\{X\}_k$：表示X经密钥K加密的结果。

基本表达式：

- $p\lhd x$：p曾看见X，P收到包含X的信息。
- $p\ni X$：P拥有或者能够拥有X。

(下转第114页)

而对范围查询，其不但使得在本地进行操作的可能性增大，而且查询的并行度也相应增加，因此变化体现得更为明显。图4表明，对于插入和删除操作，随着 N_{copy} 增加，响应性能变差，这是因为 N_{copy} 增加使得副本更新开销及相关的通信开销也相应增加。

5.2 副本数量 N_{copy} 对资源利用率的影响

资源利用率通过综合读写操作来进行模拟。图5显示，对于综合查询操作，随着 N_{copy} 的增加，CPU利用率、磁盘利用率和网络利用率都增加，这是因为 N_{copy} 增加使得副本更新开销随之增加，此外 N_{copy} 的增加还会使得任务并行可能性增大，从而增加相应的启动开销。同时还可看出，网络利用率的增加幅度比CPU利用率和磁盘利用率大，这是由于任务的启动和数据的更新都是通过信息来传递，随着 N_{copy} 的增加，其几乎呈指数上升，因而网络利用率的增加幅度最大。

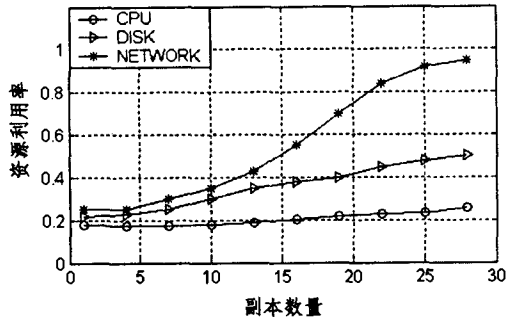

图5 副本数量对资源利用率的影响

5.3 副本数量 N_{copy} 对负载均衡度的影响

负载均衡度也通过综合读写操作来模拟。图6表明，对于综合查询操作，随着副本数量 N_{copy} 的增加，负载均衡度有较为明显的提高，特别是在副本间采用任务调度机制后。

结束语 索引复制是分布并行数据库提供并行性和提高可用性的一个重要手段，本文在 DPB$^+$-Tree 的基础上提出了相关的索引复制策略，包括副本复制原则、建立过程以及更新机制。仿真结果表明：副本对查询的响应性能有明显提高，但也相应增加了更新操作的开销；副本数量对CPU利用率、磁盘利用率和网络利用率有一定的影响；副本复制及其任务调度能够有效改善负载均衡度。

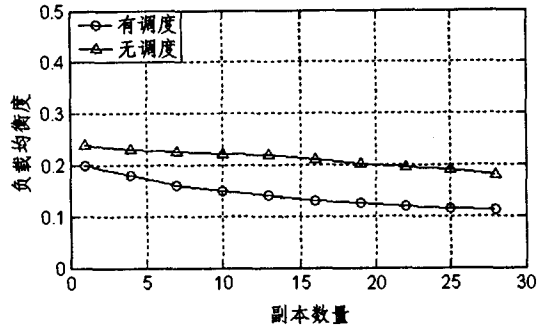

图6 副本数量对负载均衡度的影响

参 考 文 献

1 Yokota H, Kanemasa Y, Miyazaki J. Fat-Btree: An update-conscious parallel direc tory structure. In: 15th Int. Conf. on Data Engineering. Sydney, Australia, 1999. 448～457
2 Lomet D. Replicated Indexes for Distributed Data. In: Proc. of the Fourth Intl. Conf. on Parallel and Distributed Information Systems. Miami Beach, Florida, USA, 1996. 108～119
3 Devine R. Design and Implementation of DDH: Distributed Dynamic Hashing. In: Proc. of the 4th Int. Conf. on Foundations of Data Organization on Algorithms (FODO'93). Chicago, Illinois, 1993. 101～114
4 Litwin W, Neimat M-A, Schneider D. Linear Hashing for Distributed Files. In: Proc. ACM SIGMOD Conf. Washington, D. C, 1993. 327～336
5 Vingralek R, Breitbart Y, Weikum G. Distributed File Organization with Scaleable Cost/Performance. In: Proc. ACM SIGMOD Conf. Minneapolis, MN, 1994. 253～264
6 Kroll B, Widmayer P. Distributing a Search Tree Among a Growing Number of Processors. In: Proc. ACM SIGMOD Conf. Minneapolis, MN, 1994. 265～276
7 Seeger B, Larson P. Multi-Disk B-trees. In: Proc. of ACM SIGMOD Conf. 1991. 436～445
8 Litwin W, Neimat M A, Schneider D A. RP*: A Family of Order-Preserving Scalable Distributed Data Structures. In: Proc. of VLDB'94. 1994, 342～353
9 Johnoson T, Krishna P. Lazy Updates for Distributed Search Structure. In: Proc. ACM SIGMOD Conf. Washington, D. C, 1993. 337～346
10 Lomet D, Salzberg B. Access Method Concurrency with Recovery. In: Proc. ACM SIGMOD Conf. San Diego, CA, 1992. 351～360

(上接第24页)

- $p|\sim X$：P 曾发布过 X，并且 P 在发布 X 时相信 X。
- $p|\equiv X$：P 相信 X，P 认为 X 为真。
- $\#(X)$：p 表示语句 X 是新的，以前从未出现过。
- $p|\equiv\phi(X)$：P 相信 X 是可认知的。
- $\xrightarrow{k} p$：P 拥有公钥 K，相应的私钥为 K^{-1}，且不会被任何其它人知道。
- $p \Rightarrow X$：P 对 X 有控制权，P 是 X 的权威机构。
- 横线代表"推导出"，意即横线上的公式可以推导出横线下的结论。

参 考 文 献

1 Clausen T, Jacquet P. Optimized Link State Routing Protocol (OLSR). RFC 3626, 2003
2 Johnson D B, Maltz D A, Hu Y C. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). Internet-Draft, draft-ietf-manet-dsr-10. txt, July 2004
3 Perkins C, Belding-Royer E, Das S. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561, 2003
4 Zhou L, Hass Z J. Securing Ad Hoc Networks. IEEE Network, 1999, 13(6): 24～30
5 Papadimitratos P, Hass Z J. Secure Routing for Mobile Ad Hoc Networks. In: SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. (CNDS 2002). San Antonio: SCS Press, Jan. 2002. 1～10
6 Dahill B, Levine B N, Royer E, Shields C. A secure routing protocol for ad hoc networks: [Technical Report UM-CS-2001-037]. University of Massachusetts, Department of Computer Science, 2001
7 Hu Y C, Perrig A, Johnson D B. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In: Proc. 8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom2002). New York: ACM Press, 2002. 12～23
8 Hu Y C, Johnson D B, Perrig A. SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. In: Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 02). IEEE Press, 2002. 234～244
9 Marti S, et al. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks[A]. In: Proc. 6th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2000). New York: ACM Press, 2000. 255～265
10 Hu Y C, Perrig A, Johnson D B. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. In: Proc. 22nd Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2002). IEEE Press, 2003. 1976～1986
11 Li Xiaoqi, Lyu M R, Liu Jiangchuan. A Trust Model Based Routing Protocol for Secure Ad Hoc Networks. In: 2004 IEEE Aerospace Conf. Montana: IEEE press, 2004
12 Xiong Yan, Miao Fu-you, Zhang Wei-chao, Wang Xing-fu. Secure Distributed Authentication Based on Multi-Hop Signing with Encrypted Signature Functions in Mobile Ad Hoc Networks. ACTA ELECTRONICA SINICA, 2003, 31(2): 161～165
13 Capkun S, Buttyan L, Hubaux J P. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. IEEE Transactions On Mobile Computer, 2003, 2(1): 52～63
14 Burrows M, Abadi M, Needham R. A Logic of Authentication [A]. In: Proc. of the 12th ACM Symposium on Operating System Principles. Arizona, Dec. 1989
15 Gong L, Needham R, Yahalom. Reasoning about Belief in Cryptographic Protocols. In: Proc. of the 1990 IEEE Symposium on Research in Security and Privacy. IEEE Press, 1990. 234～248