一种基于移动 Ad hoc 网络的安全路由策略

蒋　毅, 史浩山
(西北工业大学 电子信息学院, 陕西 西安 710072)

摘　要: 移动 Ad hoc 网是一种新兴的无线移动自组织网络, 其路由安全机制与传统网络的路由安全机制有很大差异。在分析 Ad hoc 网络的特点和局限性的基础上, 从各网络节点易受攻击、俘获, 各网络节点之间不可信赖的角度出发, 引入了可信任第三方的信任分散策略, 提出了一种新的移动 Ad hoc 网络的安全路由策略, 解决了节点之间身份的分布式认证, 为节点之间的通信提供了极为安全的路由策略。

关键词: 移动 Ad hoc 网络; 门限方案; 分布式认证; 安全路由
中图法分类号: TP393.08　　**文献标识码**: A　　**文章编号**: 1001-3695(2005)10-0139-03

A Strategy of Security Routing in Mobile Ad hoc Networks

JIANG Yi, SHI Hao-shan
(College of Electronic & Information, Northwestern Polytechnical University, Xi'an Shanxi 710072, China)

Abstract: Mobile Ad hoc networks is a new kind of wireless mobile self-organization network. Strategies of routing security in Ad hoc networks is different from strategies of routing security in traditional network.. Based on analysing the characters and localizations in Ad hoc networks, from the perspective of fragility of security brought by the network nodes easy to be attacked, communication easy to be captured and nonconfidence between nodes, this paper presents a new strategy of security routing in mobile Ad hoc networks. The strategy is based on the technique of confidence distribution with third party, solving distributed authentication and providing security routing between nodes.

Key words: Mobile Ad hoc Networks; Threshold Scheme; Distributed Authentication; Security Routing

1　引言

目前移动 Ad hoc 网络(Mobile Ad hoc Networks, MANET)成为移动通信网络中研究的热点。移动 Ad hoc 网一改以往传统的移动通信网络需要固定的基础设施的支持及集中式的中心控制方式, 它是在无中心基础设施的情况下, 由一些移动节点组成的自组织、多跳的无线移动网络。由于没有固定基础设施的限制, Ad hoc 网一般应用于一些特殊的场合, 如军事场合、紧急突发场合、野外作业等, 现在又逐步转为民用和商用。

在 Ad hoc 网络中, 移动节点间信息的传递需要通过其他节点的多次转发才可到达目的节点, 每个节点承担主机和路由器两种功能。由于网络中各节点的频繁移动使得网络的拓扑结构在不断地变化, 在网络中传递的信息可能随时被恶意节点攻击(拦截或监听等), 网络的安全性无法得到保证。因此, 与固定拓扑结构的网络不同, Ad hoc 网络的路由随着节点的移动而不断地发生变化。如何建立路由, 保障其传输数据的安全性, 以及在路由过程中对节点进行身份认证的可靠性成为 Ad hoc 网络必须解决的问题。

基于上述 Ad hoc 网络的特点和局限性, 本文提出了一种新的移动 Ad hoc 网络的安全路由策略。该策略利用非对称加密算法建立节点间的安全路由和对称加密算法保证在 Ad hoc 网络中传递数据的安全性。由于各网络节点易受攻击、俘获, 各网络节点之间不可信赖, 所以在建立路由时要对其节点身份进行验证。为了保证用于验证节点身份的证书的可靠性, 本文借鉴 Shamir 门限方案来完成 CA 对各节点证书的分布式认证。这样既保证了路由操作的安全性, 又保证了数据传输的安全性, 防止恶意节点对路由发现过程的攻击, 确保源节点发出路由申请后可以得到目的节点一个准确而权威的路由响应。

收稿日期: 2004-10-10; 修返日期: 2004-11-23

2　相关研究

近年来国外的一些学者对 Ad hoc 网络路由的安全性问题进行了初步的研究, 与相关研究相比, 文献[1]提出了一些安全路由的机制, 但没有对 CA 的认证方案作出阐述, 而且它的路由机制存在某些安全漏洞(对节点消息来源的验证不够全面), 文献[2]提出了 CA 管理的信任分散的思想, 但并未给出信任分散的具体解决方案, 本文借鉴文献[3]的 Shamir (t, N) 门限方案给出了基于 CA 信任分散的具体分布式认证的方案。在本文提出的寻路机制及响应机制的解决方案中, 结合 CA 的分布式认证很好地解决了文献[1, 2]所存在的不足。

3　安全路由策略

3.1　设计思想

基于 Ad hoc 网络的特点和局限性所带来的问题, 本文提出的安全路由策略的内容如下:

(1) 提出了一种在 Ad hoc 网络中建立需要通信两节点间安全路由的策略, 包括寻路机制及响应机制, 同时支持安全的寻路与响应是本文的一大特点(为了保证寻路和响应的可靠

性, 加入了由 CA 支持的节点身份认证策略) 。

(2) 基于 CA 信任分散的身份认证。在 Ad hoc 网络中建立路由时, 各节点收到寻路和响应消息时, 一定先要确定消息的来源即消息的可靠性, 才可以更改自己的路由表。本文采用认证管理中心(CA) 签名的证书来认证消息来源节点的身份, 对于 CA 本文采用分散信任来保护 CA 认证的可靠性。传递消息的节点一定要在消息中附加自己的证书及签名, 消息的不可否认性才可以得到保证。对于信任分散的具体方法采用基于 Lagrange 插值公式的认证私钥分存法来实现 Shamir 门限方案, 从而完成分布式认证。

(3) 基于 Diffie-Hellman 算法的密钥交换。与在传统网络中一样, 本文同时使用两种体制来加密消息, 即用公钥(非对称) 密码体制来加密少量的关键性核心的机密数据(通常是对称加密算法的密钥) , 而对称密码体制通常被用来加密大量的数据。

本文用于加密源节点和目的节点之间传递数据的共享密钥是用基于 Diffie-Hellman 算法的密钥交换技术来实现的。由于 Diffie-Hellman 算法是基于数论中离散对数理论的难解性而设计的, 用 Diffie-Hellman 算法来交换共享密钥比在 Ad hoc 网络上直接传递加密后的共享密钥更加安全, 由此保证了数据传输的安全性。

3.2 基于 CA 信任分散的身份认证策略

3.2.1 CA 的信任分散

在公钥密码体制中, 每个节点都拥有一个公钥和私钥, 私钥是由节点自己保存的, 公钥是公开给网络上的节点共知的, 由于公钥的公开, 这就容易出现冒名攻击, 所以把所有公钥都存放在一个管理机构统一管理, 这个机构我们称为认证管理中心(Certification Authoring, CA) 。在 Ad hoc 网络中 , 两节点要进行通信时, 由于所有的节点都容易受到攻击, 也容易被俘获, 节点之间是不可信赖的, 所以在通信之前都要到 CA 询问对方的公钥、身份标志, 这些就是通常所提到的证书, 它是由 CA 统一制作并签发的。这时在军事环境中 CA 成为整个系统通信的瓶颈, 也是系统安全的薄弱点, 一旦 CA 被俘获, 整个网络也就崩溃了。本文将对一个 CA 的信任分散到多个节点, 使多个节点同时来承担信任, 以解决对 CA 安全方面的考虑。

对于一个 CA, 它具有以 RSA 算法生成的密钥对, 认证公钥(K_{CCA}) 和认证私钥(K_{PCA}) 。认证公钥是网络上任意节点所共知的, 认证私钥由 CA 自己保管。由于 CA 是系统安全的薄弱点, 所以对于 CA 认证私钥的管理是十分重要的, 攻击者可以利用认证私钥伪造节点的证书, 来攻击节点之间的信任度, 所以信任分散也就是把认证私钥的管理分散给多个节点共同承担。

3.2.2 基于 Lagrange 插值门限方案的分布式节点身份认证

我们采用 Shamir(t, N) 门限方案[3] 给出了 CA 信任分散的具体认证的方案, 用基于 Lagrange 插值公式的认证私钥分存法来实现 Shamir(t, N) 门限方案的分布式认证。其基本思想就是将 Ad hoc 中的 N 个节点作为一个认证的整体, 把 CA 的私钥分为 N 个部分, 分别由这 N 个节点共同持有, 只有当 N 个节点中的 t 个节点协同合作才可以生成认证私钥, 提供分布式认证, 而任意不超过 t 个节点是无法共同生成认证私钥的。认证私钥不是存放于单个 CA 中(实际上这里 CA 已经不存在了) , 而是以 N 个分量的形式存放于 N 个节点中, 这时会形成一个私钥分向量($k_1, k_2, k_3, k_4, \cdots, k_n$) , 对节点认证时的认证私钥可以由私钥分向量($k_1, k_2, k_3, k_4, \cdots, k_n$) 中的 t 个分量按 Lagrange 插值公式生成。

除了整个网络的密钥对(即 CA 的密钥对) , 每个节点都拥有一个密钥对, 以保证节点之间路由信息和数据信息交换的安全性。每个节点都拥有自己的证书, 证书的基本组成包括: 节点标志、节点公钥、时间戳 T(如节点 N 的证书为[$ID_N \| K_{CN} \| T$]) , 有了证书后还要用认证私钥对证书签名, 来保证证书的合法有效性, 那么这个签名的过程就是用 Lagrange 插值门限方案来进行分布式认证的过程。当有节点申请证书服务 apply 时, 每个节点利用各自拥有的私钥对私钥分向量进行 Lagrange 插值生成附加私钥($K_1, K_2, \cdots, K_n$) , 用附加私钥对 apply 进行签名(K_1[apply] , K_2[apply] , $\cdots K_n$[apply]) , 只要有 t 个节点的附加私钥对申请签名, 那么通过证书合成算法[4] , 就可以形成对节点证书的 CA 签名。这种由 N 个节点共同承担信任的方式, 使 Ad hoc 网络的认证安全性进一步提高。我们还须注意的是门限 t 值的选取要适中, 加大 t 值, 能提高系统抵抗外部攻击的能力, 但认证服务的可用性降低了; 减小 t 值, 虽然可以提高服务的可用性, 但系统就易遭受恶意攻击。

3.3 寻路机制及响应机制

3.3.1 寻路机制——路由申请的传递

当源节点 A 欲与目的节点 D 进行通信时, 如果 A 点的路由表里没有到达 D 点的可用路径, 节点 A 可以广播的方式向其邻节点发送路由申请 RREQ(Route Requests) 。

(1) 首先 A 点向其邻节点广播一个包含 RREQ 及 A 点证书的身份验证包 Request1。

$$Request1 = RREQ \| K_{PCA}[ID_A \| K_{CA} \| T_A] \| N_1 \| \#$$

其中#为路由申请的序列号, N_1 为此消息的时限, 保证消息是一个新的消息, 而不是一个旧消息的重放。

(2) 假定邻节点 B 收到 A 点的身份验证包后, 通过 CA 的公钥对 A 的证书进行验证(验证的方法就是 3.2.2 节所介绍的) 。若该证书是合法、有效的, B 点将对 A 点的身份验证包做出应答 ReRequest1, 并更新自己的路由表, 记录发送给它 RREQ 的节点 A; 若没有通过 B 点的验证, 则将 A 点的身份验证包丢弃。

$$ReRequest1 = K_{CA}[N_1]$$

(3) A 点收到 ReRequest1 后, 对其用 A 点的私钥进行解密, 确定消息的实时性(N_1) , 随后向 B 点发送一个完整的路由申请包 Request。

$$Request = RREQ \| K_{PCA}[ID_A \| K_{CA} \| T_A] \| K_{PA}[ID_A \| ID_D \| Y_A \| \#]$$

其中 Y_A 为 A, D 两点用 Diffie-Hellman 密钥交换算法计算共享密钥时 A 点的公钥。

(4) B 点收到 Request 后, 若它的路由表里没有到达目的节点足够新的路径时还会向其邻节点转发 Request 包。首先 B 发送身份验证包 Request2, C 收到 Request2, 验证 B 的身份, 并在自己的路由表里记录 B 后作出应答 ReRequest2, B 再向 C 转发 A 的 Request 包。

$$Request2 = RREQ \| K_{PCA}[ID_B \| K_{CB} \| T_B] \| N_2 \| \#$$

$$ReRequest2 = K_{CB}[N_2]$$

(5) 如果 C 点的路由表里还是没有通向 D 点的路径, 它将

把 Request 包向下继续转发直到发送到 D 点, 每一个中间节点记录第一个给它转发 Request 的邻节点, 以后再收到相同路由申请序列号的 Request 则丢弃, 若 Request 发送的中间节点本身就有一个足够新的到达 D 点的路径, Request 就不用再传递下去了, 直接记录前向节点就可以了, 通过这样的方式就建立了一条从 A 到 D 的反向路径。由于节点间只记录前向节点, 所以要通过身份验证包来确定前向节点的身份。RREQ 的传播如图 1 所示。

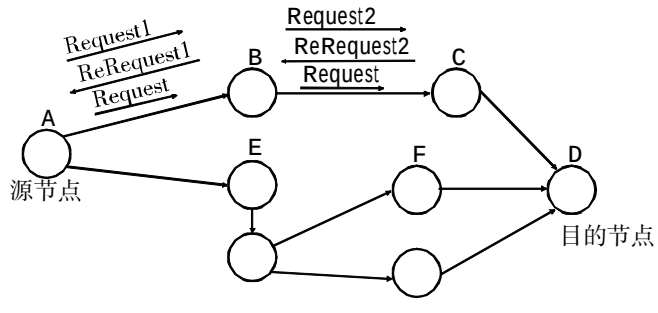

图 1　RREQ 的传播

3.3.2　响应机制——路由申请的响应的传递

当目的节点 D 收到 Request 后, 会响应第一个给它发送 RREQ 的邻节点, 向其发送响应分组 RREP(Route Reply) , 通过 RREP 的反向传递, 使路径上的节点在它们的路由表中建立起通向目的节点的正向路径。若中间节点本身就有通向目的节点足够新的路径, 由于它具有到目的节点的一部分正向路径, 则只需建立源节点到它之间的正向路径就可以了, 这种情况的响应过程与 D 点的响应过程是一致的。

(1) 假定 C 是第一个给 D 点发送 RREQ 的邻节点, 首先 D 点向 C 点发送身份验证包 Reply1, 其中包括 D 的证书。

$$Reply1 = RREP \| K_{PCA}[ID_D \| K_{CD} \| T_D] \| N_3 \| \#$$

(2) C 点验证 D 点的身份后, 作出应答 ReReply1, 并在自己的路由表里记录 D 点(这里一律假定身份验证通过) 。

$$ReReply1 = K_{CD}[N_3] \| K_{PCA}[ID_C \| K_{CC} \| T_C]$$

(3) D 点验证 C 点的身份和消息的实时性后, 向 C 点发送完整的路由请求响应分组 Reply, 若 D 对 C 的认证失败则放弃刚才接收到的路由请求包, 转去响应其他邻节点的 RREQ 请求。

$$Reply = RREP \| K_{PCA}[ID_D \| K_{CD} \| T_D] \| K_{PD}[ID_A \| ID_D \| Y_D \| \#]$$

其中 Y_D 为 A, D 两点用 Diffie-Hellman 密钥交换算法计算共享密钥时 D 点的公钥。

(4) C 点收到 Reply 后向它的前向节点 B 转发 Reply 包, 直到把 RREP 传递到源节点 A, 其他转发了 RREQ 而没有收到相应的 RREP 的节点将其路由表中先前建立的反向路径删除。

在这里可以发现后向节点发送了身份验证包后, 前向节点在应答时附加了自己的证书(这点与寻路机制不同) , 对后向节点验证身份是因为各节点要在路由表中记录后向节点, 以建立正向路径, 对前向节点的身份验证是因为 D 点只响应了一条路径的请求, 希望传递消息的路径更加可靠。图 2 是 RREP 的传播。

3.3.3　建立通信路径后的数据传输

若假定 A- > B- > C- > D, 即为 A, D 两点间建立起来的通信路径, A 点从 D 点的响应包 Reply 里解密出 Y_D(利用 CA 的公钥和 D 的公钥) 和自己的私钥 X_a 通过 Diffie-Hellman 密钥交换算法计算出 A, D 两点间的共享密钥 K_{AD}($K_{AD} = Y_D^{X_a} \bmod q$) , 同理 D 点也可以从 A 点的路由申请包 Request 中解密出 Y_A, 计算出共享密钥 K_{DA}($K_{DA} = Y_A^{X_d} \bmod q$) , 这里 $K_{AD} = K_{DA}$。这时 A 点与 D 点可以使用共享密钥传递用对称加密算法加密的大量实时数据。用 Diffie-Hellman 算法的密钥交换技术来传递共享密钥, 可以防止在 A, D 两点之传递共享密钥时易受攻击的危险(由于离散对数的难解性) 。此外, 用对称加密算法来加密数据要比用公钥加密算法传递数据时的计算简单得多, 这主要是考虑在 Ad hoc 网络中各节点的能量是有限的, 所以它的计算能力也是有限的, 过多的计算会使网络失去能量而陷于瘫痪。

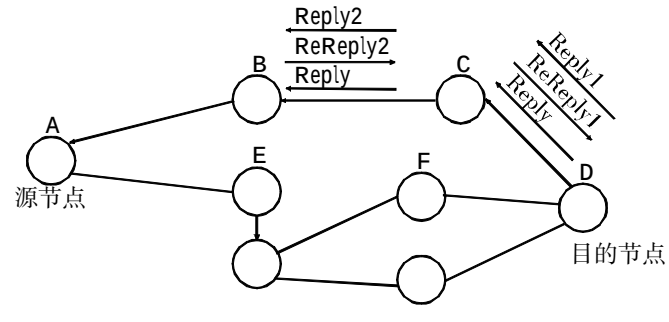

图 2　RREP 的传播

图 3 是数据的传播, 其中 $K = K_{AD} = K_{DA}$。

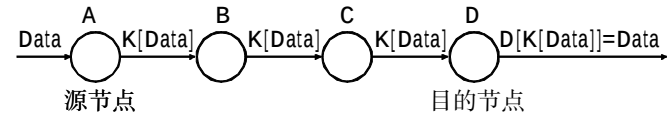

图 3　数据的传输

4　结束语

移动 Ad hoc 网络是目前新兴的一种无线移动网络, 大多用于军事领域, 安全问题是一个非常值得考虑的问题, 路由安全是整个网络安全的重要组成部分。本文构造了一种可以在移动 Ad hoc 网络环境中使用的安全路由策略, 它即可以保证路由操作的安全性, 又可以保证数据传输的安全性。这个安全策略主要是防止恶意节点对路由发现过程的攻击, 确保源节点发出路由申请后可以得到目的节点一个准确而权威的路由响应。随着移动 Ad hoc 网络向商用和民用的发展, 安全问题将持续是一个研究的热点。

参考文献:

[1]　eng Seng Ng, Seah W K G. Routing Security and Data Confidentiality for Mobile Ad hoc Networks[C] . Vehicular Technology Conference, VTC 2003-Spring, The 57th, IEEE Semiannual , 2003, 3(3) : 1821-1825.

[2]　Lidong Zhou, Haas Z J. Securing Ad hoc Networks[J] . IEEE Network, 1999, 13(6) : 24-30.

[3]　Wenjing Lou, Yuguang Fang. A Multipath Routing Approach for Secure Data Delivery[C] . Military Communications Conference, MILCOM 2001, Communications for Network-Centric Operations: Creating the Information Force, IEEE, 2001, 2(2) : 1467-1473.

[4]　Kong Jiejun, Zerfos P, *et al*. Providig Robust and Ubiqitous Security Support for Mobile Ad hoc Networks[C] . The 9th International Conference on Network Protocols(ICNP) . Riverside, California, 2001.

[5]　汤惟. 密码学与网络安全技术基础[M] . 北京: 机械工业出版社 , 2004.

作者简介:

蒋毅(1980-) , 女, 南京人, 博士研究生, 主要研究方向为数据通信和计算机网络; 史浩山(1946-) , 男, 教授, 博士生导师, 主要研究领域为多媒体通信、计算机通信网络。