文章编号:1007-5321(2010)03-0048-04

利用信任模型构建安全路由协议

余旺科, 马文平, 严亚俊, 杨元原
(西安电子科技大学 计算机网络与信息安全教育部重点实验室, 西安 710071)

摘要: 为在没有固定基站或中心节点的移动 Ad Hoc 网络中实现身份认证机制,提出了一种无需任何信任第 3 方认证服务器的动态信任模型. 在该模型中,邻居节点间通过相互认证来建立路由信息. 利用该动态信任模型组建了一个可信任的 Ad Hoc 网络. 分析结果表明,本协议增强了网络安全性,提高了路由建立效率.

关 键 词: Ad Hoc 网络; 安全; 动态信任模型; 路由协议; 认证
中图分类号: TP393.08 **文献标志码**: A

Constructing Secure Routing Protocol Using Trust Model

YU Wang-ke, MA Wen-ping, YAN Ya-jun, YANG Yuan-yuan
(Key Laboratory of Computer Network and Information Security, Ministry of Education, Xidian University, Xi'an 710071, China)

Abstract: To implement the authentication mechanism in mobile Ad Hoc networks with no fixed base station or central node, a new dynamic trust model without any third-party certification server is proposed. The neighbor nodes set up their routing information by mutual authenticating. The scheme constructs a dependable Ad Hoc networks using such dynamic trust model. Analysis results show that the new protocol enhances the security of network and increases the efficiency of routing.

Key words: Ad Hoc networks; security; dynamic trust model; routing protocol; authentication

移动 Ad Hoc 网络是一种具有高度动态拓扑结构的自组织网络,可能会导致某些节点的自私行为[1-2],给网络安全带来隐患[3]. 系统形态正从面向封闭的、熟识用户群体和相对静态的模式向开放的、公共可访问的和动态协作的模式转变. 在 Ad Hoc 网络中,没有中心化的管理权威可依赖,很难获得某一主体的全部信息,而动态信任模型在网络中的使用可解决该问题[4]. 通过对动态信任模型的研究,提出一种适合在移动 Ad Hoc 网络中运用的动态信任模型. 基于 Ad Hoc 网络按需距离矢量(AODV)路由协议[5],提出了一种在 Ad Hoc 网络中的每个节点,由自己产生公私密钥对并颁发证书的自组织动态信任管理方式下的安全路由协议.

1 动态信任模型

信任的动态性决定了信任是一个随时间和环境变化而改变的关系,A 对 B 过去的信任并不意味着现在或将来 A 对 B 会继续信任,B 的一些行为或其他一些相关信息将导致 A 对 B 的不信任. 动态信任关系模型要能反映出这种动态变化性,也要有信任随时间和环境变化而重新评估的能力. 在 A 和 B 每次交互后都要对信任度进行重新评估,如果这次交互是满意的,将调高信任值;否则,将降低信任值. 即使 A 和 B 没有发生交互,A 对 B 的信任度也会随时间的流逝而减小. 在移动 Ad Hoc 网络中的认证不适合依靠任何第 3 方认证服务中心的协助[6],所

收稿日期: 2009-07-11
基金项目: 国家高技术研究发展计划项目(2007AA01Z472); 国家自然科学基金项目(60773002)
作者简介: 余旺科(1979—), 男, 博士生, E-mail: ywkyyy@163.com; 马文平(1966—), 男, 教授, 博士生导师.

以应用于 Ad Hoc 网络的动态信任模型的构建，只能依靠节点间的相互认证来完成.

2　信任网的构建

2.1　信任度的计算

本文采用加权平均的方法对模型中的信任度进行评估. Ad Hoc 网络中的信任度会随着网络的通信时间、延迟、安全等级和负载等因素变化而增减. 各权重参数在每次证书交换认证通过后重新初始化，具体分为以下 2 个模型进行计算.

1）交换证书认证的信任度 α_i 更新计算模型为

$$\alpha_i = \begin{cases} 1 & i=1,\Delta T_1=1,\Delta R_1=1,\Delta Q_1=1, \quad \text{通过认证} \\ 0(\text{断开}) & i=1, \quad \text{未通过认证} \end{cases}$$

2）非交换证书认证的信任度 α_i 更新计算模型为

$$\alpha_i = \begin{cases} \mu(\beta\Delta T_i+\omega\Delta R_i+\delta\Delta Q_i) & \beta,\omega,\delta\in[-1,1], \quad i>1 \\ 1 & i=1 \end{cases}$$

其中

$$\Delta T_i=\frac{1}{i-1}\sum_{j=1}^{i-1}\Delta T_j$$

$$\Delta R_i=\frac{1}{i-1}\sum_{j=1}^{i-1}\Delta R_j$$

$$\Delta Q_i=\frac{1}{i-1}\sum_{j=1}^{i-1}\Delta Q_j$$

式中，ΔT 为时间权重，即 2 个节点通信时间与这 2 个节点间信任度的最近一次评估时间的差值权重，其差值越大则 ΔT 越小，说明该信任度越不可靠. ΔR 为延迟或负载权重，即 2 个节点间由于某些恶意节点进行的攻击行为或者由于在整个网络中有多条路径同时选择了经过这 2 点进行通信时的负载等因素，而导致其通信时间延长的权重，延长的时间越长则其 ΔR 值越小，说明其路径越不可靠. ΔQ 为其他因素的综合，可根据协议应用的具体环境具体考虑，本文只考虑拒绝服务等攻击行为. 如果发现某个节点进行恶意攻击行为，则将减小 ΔQ 值，使其信任度急剧下降以排除在信任网之外. 严格安全因子 μ 根据通信安全要求不同设置为 $\mu\in[0.5,1]$，当 $\mu=0.5$ 时，安全等级最高，适用于军事领域；当 $\mu=1$ 时，安全等级最低，适用于普通的商业领域.

2.2　信任等级

信任等级可根据应用环境进行设置，本文将信任等级分为以下 4 个.

1）绝对信任. $\alpha\in(0.75,1]$，即完全信任，绝对信任等级的信任列表等待更新时间为 Ad Hoc 网络中信任列表等待更新时间的 2 倍，即绝对信任等级的节点在下次的信任列表更新中不做任何处理，而只在接着的第 2 次更新才进行信任度的重新评估.

2）信任. $\alpha\in(0.5,0.75]$，信任等级的节点在每次信任列表更新时都要重新计算，并更新信任值.

3）不信任. $\alpha\in(0.25,0.5]$，不信任等级的节点在每次信任列表更新时都要重新进行证书的交换认证，如果通过认证则信任度重新设置为 1；否则信任度设置为 0.25，等下次更新时再重新进行认证.

4）不再信任. $\alpha\in[0,0.25]$，不再信任等级的节点也将在信任列表更新时重新进行证书的交换认证，如果通过认证则信任度设置为 0.75；否则信任度设置为 0，标识为断开，并广播错误报文.

2.3　信任网的构建过程

当节点 A 想加入 Ad Hoc 网络时，首先利用公钥算法产生自己的公钥 K_{A+} 和私钥 K_{A-}，并初始化自己的证书为

$$\text{cert}_A=\{\text{IP}_A,K_{A+},T_S,T_E\}$$

式中，IP_A 为 A 的 IP 地址，用作网络中节点的标识符，也可使用其他能唯一代表节点的标识符；T_S 为证书颁发时间；T_E 为证书到期时间. 最后 A 向自己的邻居节点广播探测网络邻居节点的请求报文为

$$\text{HEQ}_A=\{\text{cert}_A,T,[\text{IP}_A]K_{A-}\}$$

式中，T 是报文产生的时间戳，防止重复处理相同的 HEQ_A 报文；$[\text{IP}_A]K_{A-}$ 为 A 用 K_{A-} 对 IP_A 的签名消息. 假设 A 的邻居节点 B 收到 HEQ_A，B 首先提取 cert_A 中的数据，检测 A 的证书是否还有效. 如果有效，B 将用 K_{A+} 验证签名消息 $[\text{IP}_A]K_{A-}$. 如果验证签名所获得的 IP_A 与 cert_A 中 IP_A 相同，则 B 认为 A 拥有可信任的公私密钥对，即绝对信任 A 的存在. 接着把 B 对 A 的信任度 α_{BA} 设置为 1，再将 α_{BA} 加入 B 的信任列表 LIST_B. 最后 B 向 A 单播 1 个应答报文 HEP_A，即

$$\text{HEP}_A:\{\text{cert}_B,T,[\text{IP}_B]K_{B-}\}$$

当 A 收到来自 B 的应答报文，A 将做类似于 B 对 A 的处理步骤对 B 进行认证. 如果通过认证，A 就把对 B 的信任度 α_{AB} 也设置为 1，并将 α_{AB} 加入 A 的信任列表 LIST_A. 这样 A 与 B 就结束了相互认证的过程，A 现在相信网络中存在 1 个可信任的邻居节点 B；同时 B 也相信存在 1 个可信任的邻居节点 A. 因为 AODV 只支持双向链路，所以 $\alpha_{AB}=\alpha_{BA}$.

在经过一段证书交换认证后,A 就建立起自己的信任列表 LIST_A. 如果信任列表通过更新后由 0.5 以上的信任级别下降到 0.5 以下(包括 0.5)时,将广播路由更新报文,通知有影响的有效路由做出相应的处理. 这样就成功构建了一个可信任的 Ad Hoc 网络,如图 1 所示.

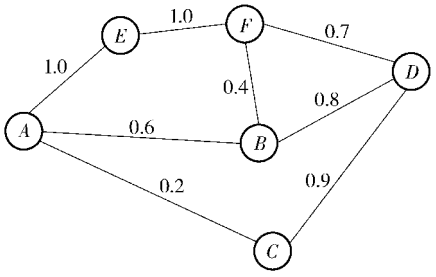

图 1 标有信任度的 Ad Hoc 网络

由于公私密钥是节点自己产生的,因此任何节点在更新密钥后重新加入网络都必须重新启动与相邻节点的相互签名认证,恢复其信任列表等信息. 与新加入信任网络的节点不同,密钥更新后的节点如果通过与邻居节点的相互认证,其信任度只能恢复为密钥更新前的信任度,而不能简单地将信任度设为 1 或其他和密钥更新前的信任度不同的值,并恢复其在密钥更新前的路径等其他相关信息. 认证失败则将其标识为断开,并广播错误报文. 这能有效防止某些信任度较低的节点或恶意节点通过更换密钥重新加入网络的办法,提高自己的信任度.

2.4 模型分析

目前已提出的动态信任模型有基于主观逻辑理论[7]的动态信任模型、基于权重的动态信任模型、基于半环代数理论的动态信任模型[8]、基于博弈理论的动态信任模型[9]等. 与其他模型相比,本文提出的信任模型主要有以下优点:① 在信任度评估中使用了公钥密码算法,使节点间的通信更安全、信任度的评估更可靠;② 规范了处于各个不同信任等级中节点的具体行为;③ 给出了节点间信任值初始化的具体方法,即通过验证的节点,其信任的初始值为 1,否则为 0. 由于本文模型中使用公钥密码算法,因此计算复杂度比其他模型略高.

3 安全路由协议

如在 AODV[5]路由协议中使用动态信任模型来构建可信任 Ad Hoc 网络,以保障通信的安全.

3.1 路由请求

如图 1 所示的可信任 Ad Hoc 网络中,各节点对应的信任列表如表 1 所示.

表 1 Ad Hoc 网络中各节点的信任列表

信任列表	A	B	C	D	E	F
LIST_A	–	0.6	0.2	0.0	1	0.0
LIST_B	0.6	–	0.0	0.8	0	0.4
LIST_C	0.2	0.0	–	0.9	0	0.0
LIST_D	0.0	0.8	0.9	–	0	0.7
LIST_E	1.0	0.0	0.0	0.0	–	1.0
LIST_F	0.0	0.4	0.0	0.7	1	–

当源节点 A 有数据包要发往目的节点 D 时,A 首先查看自己是否有到 D 的有效路由,如果没有,A 将产生一个路由请求报文 RREQ_A,并查询自己的信任列表 LIST_A(如表 1 所示). 当 A 发现只有 B 和 E 2 个邻居节点的信任度大于 0.5(LIST_A 中信任度大于 0.5 的节点,表示 A 信任或绝对信任这些节点),所以 A 只向 B 和 E 2 个邻居节点广播该路由请求报文. 而 C 的信任度只有 0.2,所以被排除在广播之外. 每个收到 RREQ_A 的中间节点(没有到 D 的有效路由的节点),将继续广播给自己信任列表中信任度大于 0.5 的邻居节点.

当 D 收到来自 A 的第 1 个 RREQ_A 时,都将等待一段时间. 在这段时间内,如果没有其他 RREQ_A 到达,D 将发出对 A 的应答报文 RREP_A. 假设途经 $A\rightarrow B\rightarrow D$ 的 RREQ_A 到达 D,且后续并没有其他请求报文到达 D,D 将应答该路由请求报文,并把相应的应答报文 RREP_A 沿反向路由 $D\rightarrow B\rightarrow A$ 单播给 A.

如果在等待时间内还有其他 RREQ_A 到达 D,如途经 $A\rightarrow E\rightarrow F\rightarrow D$ 的 RREQ_A,那么 D 将对这 2 个到达的路由请求报文的信任度进行比较,选择其中信任度较大的报文与后续收到的路由请求报文再进行比较,直到等待时间终止. 这样 D 就只对选出的具有最大信任度的路由报文进行应答,因为信任度越大,说明该路径越安全.

如表 1 所示,途经 $A\rightarrow B\rightarrow D$ 的报文信任度为

$$\alpha_{ABD}=\alpha_{AB}\alpha_{BD}=0.6\times0.8=0.48$$

途经 $A\rightarrow E\rightarrow F\rightarrow D$ 的报文信任度为

$$\alpha_{AEFD}=\alpha_{AE}\alpha_{EF}\alpha_{FD}=1.0\times1.0\times0.7=0.7$$

由于 $\alpha_{AEFD}>\alpha_{ABD}$,因此 D 只对途经 $A\rightarrow E\rightarrow F\rightarrow D$ 的路由请求报文进行应答. 当 2 个或多个路径的信任度相等时,将选择较短的路径应答. 有到目的节点有效路由的中间节点的应答,类似于目的节点的应答. 在图 1 所示的可信任的 Ad Hoc 网络中,A 与 D 间的路由建立过程如图 2 所示.

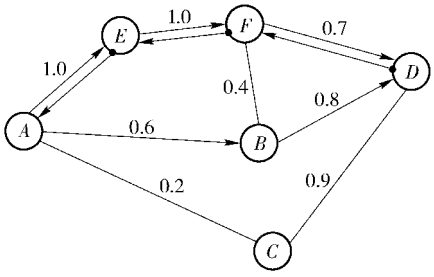

图 2　安全路由协议的路由过程

从图 2 可见，因为途经 $A\rightarrow E\rightarrow F\rightarrow D$ 的路由比途经 $A\rightarrow B\rightarrow D$ 的路由更安全，所以安全路由协议并没有选择最短的路径 $A\rightarrow B\rightarrow D$，而是选择了最安全的路径 $A\rightarrow E\rightarrow F\rightarrow D$.

3.2　路由维护

如果在应答时有途经的某对邻居节点如 $B\rightarrow A$ 时，α_{BA}的信任度从 0.5 以上下降到 0.5 或 0.5 以下时，将进行本地路由修复. 具体有以下 2 种方法：其一，节点 B 通过寻找其他有效路径进行修复. 其二，节点 B 可立即启动与 A 的证书交换认证机制，如果通过认证，将重新设置信任度为 $\alpha_{BA}=1$，并恢复该路由信息；否则设置信任度为 $\alpha_{BA}=0$，接着标志 $B\rightarrow A$ 为断开，并广播错误报文.

3.3　安全分析

在本文提出的动态信任模型中，Ad Hoc 网络中的信任度会随着网络的通信时间、延迟和负载等因素变化而增减. 如果有恶意节点进行拒绝服务攻击，其信任度会在下次信任列表更新中急剧下降，甚至把该节点排斥在信任网络外，有效防止了恶意节点进行拒绝服务攻击. 当有新的节点想加入该 Ad Hoc 网络时，该节点要取得邻居节点的信任，首先必须通过与邻居节点的相互签名认证，有效地从源头上防止了恶意节点伪装成信任节点加入信任网络，从而阻止了恶意节点进行黑洞等攻击，极大提高了信任网络的安全性. 任何节点在密钥更新后的信任度不能超过密钥更新前的信任度，有效防止了某些信任度较低的节点或恶意节点通过更换密钥重新加入网络的办法，提高自己的信任度. 另外，由于在节点信任列表的更新中，节点间的信任也是建立在相互签名的基础上，因此由此建立的信任网络能有效防止恶意节点进行报文的窃听、伪造和篡改等攻击. 这样就实现了路由报文的完整性和不可抵赖性.

4　结束语

在大部分安全路由协议中，认证或签名的算法都是应用于路由建立时，在一定程度上增加了路由建立过程的负载. 而在本文提出的安全协议中，邻居节点间的证书交换认证是发生在信任列表更新时；另外，该安全协议没有复杂的迭代计算，且具有较好的计算收敛性和扩展性，所以能有效提高路由建立效率，减少网络延迟.

参考文献：

[1] Komathy K, Narayanasamy P. Best neighbor strategy to enforce cooperation among selfish nodes in wireless Ad Hoc networks[J]. Computer Communications, 2007, 30(18): 3721-3735.

[2] 郑慧芳, 蒋挺, 周正. MANET 增强合作模型的理论研究[J]. 北京邮电大学学报, 2008, 31(5): 1-4.
Zheng Huifang, Jiang Ting, Zhou Zheng. Theoretical study with the model for MANET cooperation enforcement [J]. Journal of Beijing University of Posts and Telecommunications, 2008, 31(5): 1-4.

[3] Wang Yong, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks[J]. IEEE Commun Surveys & Tutorials, 2006, 8(2): 2-23.

[4] Song Shanshan, Hwang K, Zhou Runfang, et al. Trusted P2P transactions with fuzzy reputation aggregation[J]. IEEE Internet Computing, 2005, 9(6): 24-34.

[5] Perkins C, Belding-Royer E, Das S. RFC 3561, Ad Hoc on-demand distance vector (AODV) routing[S], 2003.

[6] 张翔, 吴荣, 汪文勇. 无线移动 Ad Hoc 网络安全认证机制研究[J]. 电子科技大学学报, 2007, 36(6): 1437-1439.
Zhang Xiang, Wu Rong, Wang Wenyong. Security and authentication mechanism research for mobile Ad Hoc network[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(6): 1437-1439.

[7] Josang A. A logic for uncertain probabilities[J]. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9(3): 279-311.

[8] Theodorakopoulos G, Baras J S. On trust models and trust evaluation metrics for Ad Hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 318-328.

[9] Yu Wei. Game theoretic analysis of cooperation stimulation and security in autonomous mobile Ad Hoc networks[J]. IEEE Trans on Mobile Computing, 2007, 6(5): 507-521.