

基于门限完全分布式密钥管理方案

沈 武,王天芹,杨 帅

(河南大学 计算机与信息工程学院, 河南 开封 475004)

摘 要: ad hoc网络作为一种无线移动网络正成为网络研究中的热点之一。针对移动 ad hoc网络的特性和对目前已有的移动 ad hoc网络密钥管理方案的分析,提出了一种基于信任图和门限密码技术的全分布、自组织的移动 ad hoc网络密钥管理新方案。该方案允许节点发布公钥证书并且通过证书链实施认证,有效地解决了网络节点之间的信任,同时又阻止恶意节点发布错误公钥证书欺骗认证服务。该方案具有较高的可靠性、扩展性和安全性,适用于大规模移动 ad hoc网络。

关键词: ad hoc网络;密钥管理;全分布;自组织

中图分类号: TP309

文献标识码: A

文章编号: 1673-629X(2010)02-0175-03

Fully - Distributed Key Management Scheme Based on Threshold

SHEN Wu, WANG Tian-qin, YANG Shuai

(College of Computer and Information Engineering, Henan University, Kaifeng 475004, China)

Abstract: The ad hoc networks is turning to be a hotspot of research. For mobile ad hoc network characteristics and available mobile ad hoc network analysis of key management scheme currently, proposed a fully distribution, self-organizing new key management scheme for mobile ad hoc networks based on trust graphs and threshold cryptography. It permits nodes to issue public key certificates and to perform authentication via certificates' chains. It is an effective solution to the trust between network nodes, in which prevent malicious nodes from issuing false certification to deceive certification services. It has higher reliability, extensibility, security, applies to the large scale mobile ad hoc network.

Key words: ad hoc network; key management; fully distribution; self-organization

0 引 言

根据文献[1]的定义,无线 ad hoc网络是由一组自主无线节点或终端相互合作而形成,独立于固定基础设施的自创造、自组织和自我管理网络。因而与有线网络相比无线链路 ad hoc网络更易于受到像主动欺骗、被动偷听、拒绝服务、冒充等安全攻击。主动攻击中恶意节点可能对路由信息进行修改;被动攻击会产生对保密信息敌意访问。由于 ad hoc网络固有的特性,传统的 PKI/CA 体制不能直接应用在 ad hoc网络中。节点频繁加入和离开网络,导致 ad hoc网络的拓扑结构是动态变化的,而且节点之间的信任关系也是变化的,必须采用动态变化的安全机制。如何在节点间建立信任关系也成为 ad hoc网络研究的难点之一,来自于网络内部恶意节点新的攻击很难防护^[2]。

在相关的文献中提出了多种确保移动 ad hoc网络

方案,主要分成两类:

(1)基于 TTP(Trusted Third Party)模型:证书和密钥由单个权威机构或者一组特别的服务节点发布,安全性依赖 CA 或固定的服务器节点。比如公钥基础设施 PKI 技术(Public Key Infrastructure)和 Kerberos。

(2)完全自组织的模型:在这个模型中,安全不依赖任何可信认证中或服务节点,像基于信任图的模型,例如 PGP(Pretty Good Private)。

我们的方案是基于第二种方法,为移动 ad hoc网络提出一种基于信任图的自组织完全分布密钥管理方案,该方案在没有可信中心和中心服务的情况下允许节点产生、存储、发布他们的公钥证书,与 PGP 相比在我们的方案中,所有的节点都是平等的,并不分配任何特别的功能给任何子节点。之所以采用这种方案是由于移动 ad hoc网络的自组织和允许节点完全控制安全设置的特性。在该方案中,节点的公私钥由节点自己产生,证书的认证是通过在信任图中的公钥证书链来完成的。证书并不像 PKI 那样存储在中心证书库中,而是由节点自己存储和发布证书。在网络中为了防止由恶意节点发布错误公钥证书,引用了门限密码机制

收稿日期:2009-06-23;修回日期:2009-09-06

基金项目:国家自然科学基金资助项目(10671056)

作者简介:沈 武(1979-),男,安徽人,硕士研究生,研究方向为密码学和信息安全;王天芹,教授,研究方向为密码学和数论。

(n, t) 。

1 相关研究

1.1 部分分布式 CA (partially distributed CA)

部分分布式 CA 方案是由 Zhou 和 Haas^[3]提出。该方案采用分布信任机制和门限密码机制 (n, t) , 将 CA 私钥分成 n 份私钥份额, 分发给 n 个服务节点, 其中任意 t 个联合起来可以执行 CA 功能。签发证书时, CA 节点生成部分签名证书, 由一个联合节点重构完整的签名证书。Yi 和 Kravets 的 MOCA 认证方案^[4]对 Zhou 的方案作出了改进, 取消了组合节点, 并提出了证书撤销机制, 通过缓存路由减少了通信代价。Zhang 等人提出基于 ID 的门限密钥管理方案^[5], 节点的公钥是由已知 ID 和一些普通信息组合, 该方案消除了公钥证书发布。Deng 等人提出了基于族结构方案, 系统把网络分成多个族, 每个族中由族头维护一张 CA 信息表, 表中包括族内信息表和其它族的信息表。部分分布式 CA 方案将单一的 CA 服务分散到 n 个节点中, 有效地防止了单点失败, 提高了网络的抗攻击能力。

缺点是:

(1) 节点需要到 t 个认证节点去申请证书, 这些节点可能遍布于网络各处, 需要多跳通信才能达到, 增加了网络的通信负荷;

(2) 认证节点的计算量和通信量都非常大, 容易造成通信瓶颈;

(3) 门限机制中的参数 n 体现了方案的可用性, t 体现了方案的安全性, 选择合适的 n 和 t 并不容易。

1.2 完全分布式 CA (fully distributed CA)

完全分布式 CA 方案中 CA 的任务由所有网络节点共同承担, 每个节点都持有部分私钥, 任意 t 个节点联合可以执行 CA 功能, 因此提高了系统的可用性。PGP 是一个完全分布式方案, 最初为 e-mail 提供安全, 它允许多个用户推荐一个用户签名它的公钥证书, PGP 采用了网状信任的系统模型, 不需要 CA 的存在。但是这种模型并不是完全安全的, 因为不诚实的用户可能发布错误的证书欺骗其它用户。基于相同的原理, Capkun 等人提出了自组织的移动 ad hoc 网络信任模型^[6], 节点之间的信任是通过物理的方法构造的, 在这种模型中每个节点在他自己信任范围内给其它节点发布公钥证书, 节点通过信任链相互认证。该方案的另一个特点是门限值可以在系统运行过程中随着网络节点数量的变化而动态改变, 具有可扩展性。缺点是:

(1) 证书的处理需要多个节点的参与, 将部分签名组合成一个完整的签名, 计算比较复杂, 因此效率并不是很高;

(2) 方案假设每个节点周围都至少有 t 个节点, 并不是所有情况下该条件都会成立;

(3) 网络中的每个节点都是 CA 节点, 攻击者可以攻击任意 t 个节点, 从而降低了系统的安全性。

2 背景知识

(1) Shamir (t, n) 门限秘密分享方案。

Shamir (t, n) 门限方案 $(t \leq n)$ 是基于多项式的 Lagrange 插值公式的密码技术, 把密钥 S 分成 n 个互不相同的子密钥 S_i , 因此需要知道至少 t 个共享子密钥才能恢复初始密钥 S 。可信方 T 的秘密信息 $S \in Z_q$, 该方案具体如下:

· 初始化阶段:

a. T 选择秘密多项式 $f(x) = S + \sum_{j=1}^{t-1} a_j x^j \pmod{q}$ $q \in Z_q[x]$, 其中: $a_j \in_R Z_q, j = 1, 2, \dots, t-1$ 。

b. T 计算 $S_i = f(P_i) = S + \sum_{j=1}^{t-1} a_j P_i^j \pmod{q}$ 并将 S_i 秘密送给 $P_i \in P (i = 1, 2, \dots, n)$ 。

其中: P 是由节点 P_1, P_2, \dots, P_n 组成的集合, P_i 是节点标志。

· 恢复密钥阶段:

a. 任意 t 个参与者(组成集合 B) 可以通过公式 $S = \sum_{P_i \in B} C_{B_i} S_i \pmod{q}$ 重构 S 。其中:

$$C_{B_i} = \prod_{P_j \in B \setminus \{P_i\}} [p_j / (P_j - P_i)] \pmod{q}$$

b. 对于 $P_j \in B$, 集合 B 能通过 $S_i = \sum_{P_j \in B} C_{B_j} (P_j)$ $S_i \pmod{q}$ 计算 P_j 的共享份额。其中:

$$C_{B_i} (P_j) = \prod_{P_l \in B \setminus \{P_i\}} (P_j - P_l) / (P_i - P_l)$$

3 方案实现

最初在 PGP 和文献[7,8]中的信任关系是基于以下的方式: 如果 A 相信 B , B 又信任 C , 那么 A 就信任 C 。根据这种信任关系, 信任链中易攻击的点主要是 B , 如果 B 被攻破, 那么所有经过 B 的链路可能都是不正确的。基于这种考虑, 提出更安全的概念: 如果 A 相信 B , B 又信任 C , 那么, 如果其它 $k-1$ 个可信的节点信任 B , 那么 A 就信任 C 。通过这种方式, A 能通过系统中其它可信节点的联合来观察 C 的行为。为了提供信任共享, 方案采用了 (k, n) 门限方案, n 是系统中的节点的数量, $k < n$ 是信任度。

(1) 初始化阶段。

初始化阶段一: 每个节点从秘密分发者 T 处通过安全的渠道获得各自的私钥共享份额。

a. T 选择秘密多项式 $f(x) = S + \sum_{j=1}^{t-1} a_j x^j \pmod{q}$ ($q \in Z_q[x]$), 其中: $a_j \in_R Z_q$, $j = 1, 2, \dots, t-1$ 。

b. T 计算 $S_i = f(P_i) = S + \sum_{j=1}^{t-1} a_j P_i^j \pmod{q}$ 并将 S_i 秘密送给 $P_i \in P$ ($i = 1, 2, \dots, n$)。

其中: P 是由节点 P_1, P_2, \dots, P_n 组成的集合, P_i 是节点标志。

初始化阶段二:部分证书的构造,所有的节点获得他们各自的私钥共享份额后,每个节点给他们互相信任的成员产生部分证书,这样就构造了由部分证书构成的特别信任图。假定在初始化节点之间不存在信任关系,那么系统就变成了完全分布的模型而且没有基础设施,初始化以后 T 将离开系统。

(2) 节点的加入。

系统初始化后进入运行阶段,当出现一个新节点要加入网络时,将执行下面两步操作:第一步:新节点与当前任何其相邻的节点取得联系,发送加入系统的请求。在这个过程中,相应的成员节点(称代理节点)将处理节点加入请求。首先新节点自己产生公私钥对 PK/SK ,然后把 PK 和可信证明发送给代理节点,请求由系统私钥为其公钥签名的证书。为了认证由新节点提供的可信证明,代理节点向其它的成员节点发送请求。如果信任证明被某个成员节点认证,那么该成员向代理节点发送由这个成员的私钥共享签名的部分证书。这个过程持续,直到代理节点获得至少 t 个不同的成员的私钥共享签名的部分证书为止。然后结合产生包含新节点的公钥的完整的证书。第二步:改变方案的配置,从 (t, n) 到 $(t, n+1)$ 。与第一步不同,第二步不需要代理节点的参与,只有新节点操作。在这步中,包括新节点的部分私钥共享,用新成员的公钥加密的信息交换。首先,新节点 i 用他的私钥签名的请求在网络中广播,一旦成员 j 收到请求,然后为他计算部分私钥共享, $S_{i|j} = S_j l_j(i) + \Delta_j \pmod{q}$, Δ_j 是为了阻止 S_j 的泄露; $l_j(i) = \prod_{r=1, r \neq j}^t \frac{i-r}{j-r} \pmod{q}$ 。每个成员节点返回一个用新节点的公钥加密的部分私钥共享发送给新成员节点。新节点在收到 t 个部分私钥共享份额后,新节点能构造他自己的私钥共享, $\sum S_{i|j} = S_i \pmod{q}$, 至此,新成员已经变成了网络中的成员并且参与证书管理。

(3) 证书交换和公钥认证。

在我们的方案中,部分证书的交换是一种重要的机制,让节点共享和发布他们持有的部分证书,部分证书交换协议定期地在每个节点以及相邻节点之间执行,在这个阶段,移动 ad hoc 网络的动态特性允许节点

从其它的节点恢复更多的知识,建立大量的部分证书并且更好地评价部分证书的相关性。

方案使用由部分证书链组成的特别部分信任图。部分信任图由有向图 $G < V, E >$ 表示, V 代表节点标识符, E 代表部分证书。如果存在由 i 的私钥共享为 j 签名的证书,其中证书包括 j 的标识符和 j 的公钥 k_j , 那么就存在一条从 i 到 j 的有向边,从节点 i 到 j 部分证书链由 G 中的从节点 i 到 j 的一条有向路径表示。因此,如果在 G 中任何两个节点被连接,就代表存在一条证书链。

节点之间的公钥认证是通过部分证书链的合并来完成的。当一个节点 i 需要认证另一个节点的公钥 j 的公钥时,两个节点合并并验证他们的部分信任图。合并图的验证是通过部分证书的签名的合并来完成的。两个节点 i 和 j 在部分信任图中相互验证完成证书签名,如果验证成功,所有的节点的入度边被标记为可信的边;否则,签名联合失败,所有的入度边被删除。然后节点 i 向节点 j 试着找出一条信任链,如果这样的链找到,认证完成,节点 i 相信节点 j 的公钥。

4 安全分析

通过考虑网络中的恶意节点来验证方案,这里区别两类攻击:内部恶意节点和外部恶意节点攻击。在方案中外部节点没有途径假冒成员节点,成员节点能够通过检查他们的证书合法性来验证他们的身份。并且能够签名部分证书的节点必须拥有其门限密码方案相应的私钥共享,同样外部节点也没有途径签名伪造部分证书。

内部恶意节点可能发布多种类型的错误证书:

(1) 为了欺骗其它的节点相信某个伪造的绑定,它可能发布一个证书,该证书把公钥 K_i 绑定节点 j 取代节点 i 。

(2) 它还可能发布一个证书,该证书把节点 j 绑定到伪造的公钥 K'_j , 然后可能造成其它的节点相信这个伪造的绑定。

(3) 它能编造许多节点身份和公钥并且用适当的证书绑定它们。

我们的方案能抵抗以上描述三类绑定。如果一个恶意的成员想要编造一个伪造的绑定,那么他必须最少存在 $k-1$ 个部分证书。然而,要做到那样,敌手成员必须从合谋成员收集最少 k 个私钥共享,同时要签名 k 个伪造证书。而且,像上面(3)所提到的,恶意的节点没有任何途径欺骗其它的节点相信一个伪造的部分信任图,因为合并信任图要被删除所有未能使用系统

(下转第 181 页)

控制的 TCP 流不能公平地获取带宽。

据此,对基于路由器的拥塞控制算法提出改进:

(1)针对无反应的 UDP 攻击流。当网络中 TCP 流与 UDP 流共存时,需要基于网络的机制来减小因失控和高速 UDP 流量负荷而导致的拥塞崩溃效应。换句话说,因为 UDP 发送者不能够检测拥塞,所以像使用包队列和丢弃技术的路由器这样的网络基本设备往往就成为降低 UDP 过大通信量的有效工具。可以设计 UDP 拥塞控制协议,通过在诸如流媒体类型的高速率 UDP 流中增加主机拥塞控制来减小这个潜在的问题,这是目前网络拥塞控制的研究热点之一。

(2)针对恶意的 DDoS 攻击流。相关的研究表明,在路由器中根据 DDoS 攻击包的特征来识别和隔离攻击流有很大的困难。然而,可以根据上述的 DDoS 攻击流的协议行为(DDoS 攻击数据流在发生网络拥塞的情况下并不降低它们的发送速率,充满了路由器的缓冲区,剥夺其他正常数据流的带宽),改进路由器的拥塞控制算法。改进的机制为当一个数据包进入路由器后,算法对被鉴别出的高带宽流的数据包先进行一次提前丢弃,未被丢弃的包将进入 RED 的输出队列,而非高带宽流的数据包不用通过这个提前丢弃处理,直接进入 RED 队列。此机制通过提前丢弃高带宽的数据流,可实现带宽分配的公平性。

5 结束语

RED 算法已成为路由器中的默认拥塞控制机制,

它能较好地解决全局同步问题和对突发性业务的服务特别差的问题,却不能有效隔离恶意破坏的用户和对丢失不够敏感的用户。而目前,随着攻击流和非响应流的增多,它们给未来的网络带来了很大的威胁,迫切需要解决这种数据流的机制和措施。

参考文献:

- [1] 杨凯峰,洪佩琳,束永安,等. Internet 路由器中的拥塞控制策略[J]. 小型微型计算机系统,2000,21(5):353-356.
- [2] 仲 燕,孙知信. 路由器防范拒绝服务攻击技术研究[J]. 南京邮电学院学报,2005,25(6):90-94.
- [3] Garher L. Denial-of-Service Attacks Rip the Internet[J]. Computer,2000,33(4):12-17.
- [4] Lee R B. CE-L 2003-003, Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures[R]. Department of Electrical Engineering, Princeton University,2003.
- [5] 忽海娜,冯 浩,王中立. DDoS 攻击下高带宽聚类的控制[J]. 计算机技术与发展,2008,18(4):155-157.
- [6] Braden B, Clark D. Recommendations on Queue Management and Congestion Avoidance in the Internet[S]. RFC2309. Network Working Group,1998.
- [7] Floyd S, Jacobson V. Random early detection gateways for congestion avoidance[J]. IEEE/ACM Transactions on Networking,1993,1(4):397-413.
- [8] 徐雷鸣,庞 博,赵 耀. NS 与网络模拟[M]. 北京:人民邮电出版社,2003.

(上接第 177 页)

公钥联合签名的节点验证。

5 结束语

在该方案中,在没有任何 TA 的情况下,提出了一种完全分布自组织公钥管理方案。我们的方案是基于信任图,其中为了抵抗恶意的节点发布错误公钥证书欺骗认证服务,还使用了著名的门限方案。我们的方案是分散和完全分布式的,是专门为移动 ad hoc 网络设计的。其一个重要特征是,当网络分割和节点仅能和其它一部分节点通信时,公钥认证仍然是可行的,因此更合适大规模移动 ad hoc 网络。

参考文献:

- [1] Perkins C E. Ad Hoc Networking[M]. [s.l.]: Addison Wesley Professional,2000.
- [2] Deng H, Li W, Agrawal D P. Routing security in wireless ad hoc networks[J]. IEEE Communications Magazine,2002,40

(10):70-75.

- [3] Zhou L, Haas Z. Securing ad hoc networks[J]. IEEE Net, 1999,6(13):24-30.
- [4] Seung Yi, Kravets R. Moca: mobile certificate authority for wireless ad hoc networks[C]// In Proceedings of 2nd annual PKI research workshop (PKI03). Gaithersburg, MD, USA: [s.n.],2003.
- [5] Zhang Y, Liu W, Lou W, et al. Securing mobile ad hoc networks with certificateless public keys[J]. IEEE Trans Dependable Secure Comput,2006,3(4):386-399.
- [6] Capkun S, Buttyan L, Hubaux J. Self-organized public-key management for mobile ad hoc networks[J]. IEEE Trans Mobile Comput,2003,2(1):52-64.
- [7] Capkun S, Buttyan L, Hubaux J. Small worlds in security systems:an analysis of the PGP certificate graph[C]// In Proceedings of the 2002 workshop on New security paradigms. [s.l.]:ACM Press,2002:28-35.
- [8] Ren K, Li T, Wan Z, et al. Highly reliable trust establishment scheme in ad hoc networks[M]. [s.l.]: Elsevier, 2004.