

文章编号:1001-9081(2005)12-2727-04

移动 Ad Hoc 网络中的组密钥管理策略

张桢萍,许 力,叶阿勇

(福建师范大学 计算机科学系,福建 福州 350007)

(chazhzhp@fjnu.edu.cn)

摘要: 移动 Ad Hoc 网络是由移动节点组成的不需要固定基站的临时性计算机通信网络,设计这种网络的主要挑战之一是它们在抵抗安全攻击方面的脆弱性。无中心、动态拓扑和时变链路使得移动 Ad Hoc 网络的组密钥管理面临巨大的挑战。通过对现有的组密钥管理策略进行对比分析,为该领域的进一步研究提供了思路。

关键词: 移动 Ad Hoc 网络;组密钥;组播

中图分类号: TP309 **文献标识码:**A

Group key management strategy of mobile Ad Hoc network

ZHANG Zhen-ping, XU Li, YE A-yong

(Department of Computer Science, Fujian Normal University, Fuzhou Fujian 350007, China)

Abstract: Mobile Ad Hoc network is a collection of wireless mobile nodes forming a temporary computer communication network without the aid of any established infrastructure, and one of the challenges in designing the kind of network is the fragility in withstanding the attacks of security. The group key management of mobile Ad Hoc network is facing a great challenge because of its acebtric, dynamic topology and realtime changed link. By comparing and analyzing the strategy of group key management in existence, it provides an idea of the further study in this field.

Key words: mobile Ad Hoc network; group key; multicast

0 引言

移动 Ad Hoc 网络是一种新型的无线自组织网络,它不依赖于任何事先铺设的固定设施,由一组自主的无线节点或终端临时组成,该网络中的功能主要通过移动节点之间的相互协作完成^[1]。

由于移动 Ad Hoc 网络共享无线信道,因此它具有自组织、多跳、动态拓扑、临时组网等特性。然而,它的缺点也是显而易见的:拓扑结构变化频繁容易导致路由失败、无线带宽资源有限、无线通信信道可靠性不高、易受无线通道的噪音干扰、基础设施的缺乏、计算和存储能力有限、节点的脆弱性(移动的、未受保护的)等。

移动 Ad Hoc 网络自身的特殊性决定了它将面临与传统无线网络相同甚至更严重的安全问题,其中组密钥管理策略的研究是当前的一个热点和难点。在无中心的移动 Ad Hoc 网络中,每个节点的身份是对等的,并且由于网络中不存在任何一个完全可信的实体,移动节点之间的会话密钥必须由需要通信的节点双方自行产生。因此,移动 Ad Hoc 网络面临着许多新的安全威胁,要求采取有效的安全措施^[2]。

组密钥是所有组成员都知道的密钥,被用来对组播报文进行加密/解密、认证等操作,以满足保密、组成员认证、完整性等需求。密钥管理系统包括密钥的生成和维护,密钥维护指的是由于成员节点的加入和退出而改变密钥,或者由于长时间使用后需要对组密钥进行更新。

组密钥管理策略应具备的一般属性有:可扩展性、可靠

性、能量保护性^[1]。而由移动 Ad Hoc 网络的特殊性,决定了还应该对组密钥管理策略的安全属性提出一些特定的要求^[3],具体地说,它除了要包括有效性、保密性、完整性、认证性和不可否认性(即责任认定性)外,还需要解决以下几个基本问题:

(1) 安全性,包括前向安全性和后向安全性。前向安全性指当节点退出时,需要更新 TEK(Traffic Encrypt Key,组通信密钥),以保证退出的节点不可能再获得组通信信息;后向安全性指节点加入时,需要更新 TEK,以保证新节点不能获得已经传输的信息。

(2) 同谋破解。组播密钥管理不仅要防止某个节点破解系统,还要防止某几个节点联合起来破解,因此要杜绝同谋破解或降低同谋破解的概率。

(3) 组密钥管理策略的可扩展性。可扩展性包括密钥发布占用带宽、密钥发布的延迟以及密钥生成计算量等。具体的说,要求密钥更新报文不应占用过多的网络带宽;密钥更新时要使所有组成员都能及时地获得新的密钥;同时,由于通常情况下协同的密钥生成需要较大的计算量,计算复杂度较大,因此当节点的计算资源不充足或密钥更新频繁时,要考虑密钥生成给节点带来的负载。

(4) 密钥通信代价。节点的耗能除了计算耗能外,还包括通信耗能,而通信耗能远远大于计算耗能。

(5) 健壮性。当部分组成员失效时,不会影响安全组播的继续工作。

(6) 可靠性。当网络环境不可靠时,确保密钥分发与更

收稿日期:2005-06-27 基金项目:国家自然科学基金资助项目(60372107);福建省自然科学基金资助项目(A0440001)

作者简介:张桢萍(1979-),女,福建连城人,助教,硕士研究生,主要研究方向:无线 Ad Hoc 网络、网络与信息安全; 许力(1970-),男,福建福州人,副教授,博士,主要研究领域为:无线网络与移动计算、网络与信息安全; 叶阿勇(1977-),男,福建漳州人,讲师,硕士,主要研究方向:网络与信息安全。

新仍然能够正确实行。

判断策略好坏的标准还需要在复杂性和安全性两方面均衡考虑,而且在具体应用中,密钥管理策略对于上述基本问题的要求程度也有所不同。

对于组播密钥管理策略,可以根据网络的拓扑结构进行分类,也可以根据所使用的算法类型进行分类,甚至可以根据某项技术的使用与否进行分类。由于拓扑的动态变化是移动 Ad Hoc 网络的主要特征之一,本文按照网络的拓扑结构将组播密钥管理策略分为集中式、分布式和分层分组式三大类。

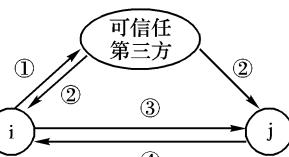
1 集中控制式组密钥管理策略

移动 Ad Hoc 网络作为末梢网,是与有基础设施的网络相连的,它可以指定主干网络中的节点作为第三方认证服务器来提供认证服务。正是由于这一点,它才可以采用传统网络中的集中式管理策略,即采用单个节点统一提供整个网络的认证服务。

传统的集中式控制方式的认证过程是单向的,即只有网络的中心机构对移动节点进行认证,而移动节点对网络的中心机构不作认证,并且移动节点之间建立会话密钥时必须通过可信任的第三方(如网络的中心机构)。如图 1 所示。

图 1 中,节点 i 希望与节点 j 建立通信,则:

① i 将 REQ_{ij} 送到可信任的第三方,请求与 j 建立通信;



② 可信任第三方接收 REQ_{ij} 后,送 k_{ij} 到 i, j ,用于 i, j 之间进行通信;

③ i 接收到 k_{ij} 后,与 j 建立通信,发送 $C = E_{k_{ij}}(M)$ 给 j ;

④ j 收到 C 后,用 k_{ij} 解密: $M = D_{k_{ij}}(C)$ 。

密钥更新与上述密钥生成类似,假设节点 i 希望更新自己与节点 j 的通信密钥,则它向可信任第三方发送密钥更新的请求;可信任第三方收到节点 i 的请求后,将产生一个新的密钥 k'_{ij} 并发送给节点 i 与 j 。

集中式认证方式的认证模型主要有基于对称密钥的 KDC(Key Distribution Center, 密钥分配中心)模型和基于非对称密钥的 PKI(Public Key Infrastructure, 公钥系统)模型。KDC 模型在可信任的第三方认证服务器如 KDC 上保存通信双方的密钥,以此提供在线的认证服务。而 PKI 模型采用可信任的第三方认证服务器如 CA(Certificate Authority, 认证中心)为节点颁发证书来提供认证服务,节点则使用 CA 颁发的证书来建立和其他节点之间的信任关系。

文献[4,5]提出了一个简单的采用集中控制的组播密钥管理策略 GKMP(Group Key Management Protocol, 组密钥管理协议)。文献[6]描述了应用于集中控制方式的逻辑密钥树,对于一个中间节点子节点个数为 k 、层数为 $d+1$ 的平衡逻辑密钥树,组控制器保存的密钥个数为 $(k^{d+1}-1)/(k-1)$,这将导致组控制器需要很大的密钥存储空间来支持大规模的组播,并将增加密钥操作的运算量,文献[7]提出了一种可以降低组控制器保存的密钥数的方案。另外,由于减少密钥更新所需要发送的信息量可以降低密钥更新延迟和占用的带宽,因此文献[8,9]分别给出了两种方案使二叉密钥树的密钥更新网络流量由 $O(2\log n)$ 降为 $O(\log n)$ 。

2 分布式组密钥管理策略

集中式中的 CA 实际上是一个可信任的实体,但是在在一个移动 Ad Hoc 网络中仅仅利用一个 CA 完成密钥管理服务具有脆弱性,因为一旦该 CA 失效,网络中的节点将不能获得其他节点的公钥,也不能建立与其他节点之间的安全通信。如果 CA 被敌对节点攻破,敌对节点将能够用截取的私钥对假冒的证书进行签名,并且能够模仿任何其他的节点或者撤销任何已经发放的证书。

改进服务的有效性的一般方法就是对 CA 进行复制,但是这种简单的复制将会导致脆弱性的提高,因为复制品越多,被攻破的可能性就越大。为了解决这个问题,于是出现了将信任分发到一个节点集的方法,让这些节点共同分担密钥管理的职责。

分布式策略通常采用文献[10]提出的门限共享加密技术。该技术基于以下假设:在自组网中,没有任何一个单独的节点是值得信任的,但认为一个节点的集合是可信任的。一个 (n, t) 门限方案是一种在 n 个参与者中分享一个密钥 k 的方法,使得任意 t 个参与者在给出他们的秘密份额后可以恢复密钥 k ,而任意 $t-1$ 个参与者在给出他们的秘密份额后不能恢复密钥 k 。根据共享密钥时节点选择的不同,分布式策略可分为部分分布式和完全分布式两种。

2.1 部分分布式

部分分布式认证方法最早由文献[3]提出。在该认证方法中,网络由服务节点和普通客户节点组成。每个节点拥有自己的公钥和私钥,并且能够提交查询请求以获得其他节点的公钥,也能提交更新请求以改变它们自己的公钥。而每个服务节点则保存了网络中所有节点的公钥。

网络中需要一个管理机构创建网络并给待加入的节点发放有效证书。初建网络时,管理机构负责实现网络的初始化,同时选择最初的 n 个服务节点(网络中节点的总数为 N),并利用 (n, t) ($t > 1, n \geq 3t - 2$) 门限共享加密技术将证书密钥共享。当新节点加入时,由网络中的 t 个服务节点产生部分证书发送给新节点,从而实现密钥在全部节点间的共享。

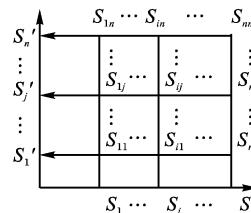
(1) 部分分布式策略中证书共享的步骤如下:

① 选择一个素数 p ,并由管理机构产生一个共享多项式:

$$f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$$

其中, $a_0 = SK, SK$ 是 CA 的私钥, $a_i (i = 1, 2, \dots, t-1)$ 可从 Z_p 中随机选取。

② 最初的 n 个节点记为 $v_i (i = 1, 2, \dots, n)$,它们获得的共享密钥为 $s_i = f(v_i) \bmod p$ 。



(2) 部分分布式策略中证书更新的步骤如下:

① 更新多项式 $f'(x) = b_0 + b_1x + \dots + b_{t-1}x^{t-1}, f'(x)$ 中常数项为 0。每个服务节点产生一个密钥为 0 的 (n, t)

图 2 部分分布式认证的证书更新 随机共享,也称为子共享,同时将这些子共享分发给其他的服务节点,用 s_{ij} 表示节点 i 发送给节点 j 的子共享。

② 节点 j 的 n 个子共享记为 $s_{ij}, i = 1, \dots, n$,这样节点 j 的更新密钥为 $s_j' = s_j + \sum_{i=1}^n s_{ij}$ 。如图 2 所示。

此外,由于每个服务节点都保存了网络中所有节点的公

钥, 网络中的节点通信时只需要请求一个服务节点就行了。可见, 部分分布式认证策略中, 密钥管理服务被分布到网络中的多个节点, 实现信任的分散; 同时由这些节点共同承担 CA 的认证功能, 实现风险和负担的分解, 避免了单个节点充当中心节点带来的隐患, 从而保证安全的密钥管理服务。

2.2 完全分布式

完全分布式认证最早由文献[11]中提出, 文献[12, 13]中给出了进一步的分析。在完全分布式策略中, 节点独立维护自己的密钥, 会话钥匙由参与会话的所有节点按某种协议分布协作生成, 且要经常改变。与部分分布认证不同的是, 它利用 (n, t) 门限共享加密技术将一个 RSA 证书签名密钥分发给网络中的所有节点。

网络的初始化和部分分布认证方法相似, 管理机构此时选择 t 个节点共享密钥, 网络建成后由网络中的节点开始充当 CA 的功能。每个节点在加入到网络之前必须从管理机构处获得最初的有效证书。网络的初始化完成后, 管理节点随之消失, 不再参与移动 Ad Hoc 网络中的其他操作, 从而保证了移动 Ad Hoc 网络的无中心节点的特性, 并有效地确保了网络安全。

(1) 完全分布式策略中新节点加入时的证书共享

假设有一个新的节点 v_i 加入, 它必须交换证书以获得与新的邻居节点的信任关系。如果 v_i 节点仍未初始化, 则它首先获得 t 个节点的组合 $B = \{v_1, v_2, \dots, v_t\}$ 。

① v_i 将初始化请求与 B 中 t 个节点的 ID 广播到网络中。

② 当节点 $v_j \in B$ 接收到请求后, 检查 v_i 的证书和证书取消列表(Certificate Revocation List, CRL), 如果 v_j 决定响应请求, 则它为 v_i 计算得到一个部分证书:

$$P_j = P_{v_j} l_{v_j}(v_i) \bmod p$$

其中 P_{v_j} 是 v_j 自身的部分证书, 并且 $l_{v_j}(v_i) = \prod_{r=1, r \neq j}^t$
 $\frac{v_i - v_r}{v_j - v_r}$, p 是两个大素数 p_1, p_2 的乘积: $p = p_1 \cdot p_2$ 。

③ 如果 v_j 只是向 v_i 返回部分证书 P_j , 那么 v_i 能够通过组合收到的 t 个部分证书而得到一个完整的证书。由 Lagrange 插值多项式可得:

$$P_{v_i} = f(v_i) = P_{v_1} l_{v_1}(v_i) + P_{v_2} l_{v_2}(v_i) + \dots + P_{v_t} l_{v_t}(v_i) \\ = \sum_{j=1}^t P_{v_j} l_{v_j}(v_i) = \sum_{j=1}^t P_j \bmod p$$

但是这种证书共享方式存在着一个严重的安全隐患, 因为节点 v_i 通过 P_j 可以很容易得到 v_j 的认证私钥分量 P_{v_j} 。文献[11]中对其进行了详细的分析并给出了一个解决方法, 该方案能够实现不让 v_i 得到单个 P_j 。首先节点 v_i 预先通过广播方式得到愿意给它提供服务的 t 个节点的集合 $B = \{v_1, v_2, \dots, v_t\}$, 然后集合 B 中的每个节点将它们各自的部分证书完全打乱后再送还给节点 v_i , 从而保证 v_i 不能得到单个 P_j 。

(2) 完全分布式策略中证书的更新

为了尽可能地防止网络中节点的证书被恶意节点非法截取, 必须定时对证书进行更新。证书更新的步骤如下:

① 节点 j 需要更新它的证书时, 向其一跳节点发送证书更新请求。

② 节点 i 收到请求后, 首先验证节点 j 的证书是否有效, 如果有效, 则应用 $cert_i(cert)^{P_i}$ 生成部分证书; 然后节点 i 随机产生数 u , 计算 $A_1 = g^u$ 和 $A_2 = cert^u$, g 为 Z_p 的生成算子, 并计算哈希函数 $c = Hash(g^{P_i}, cert, A_1, A_2)$, $r = u - c \cdot P_i$; 最后节

点 i 将 $cert_i, A_1, A_2$ 和 r 发送给节点 j 。

③ 节点 j 选择 t 个部分证书。选择的过程中通过验证 $cert^r \cdot (cert_i)^c = A_2$ 的成立与否判断收到的信息是否来自有效的节点。若未通过验证, 则发送该无效证书的节点将被取消, 直到找到 t 个部分证书。

④ 节点 j 将选择的 t 个部分证书作如下结合:

$$cert_{new} = \prod_i (cert_i) l_{v_i}(0)$$

该策略中假设网络中的每个节点都至少有 t 个行为好的合法节点, 因此 t 是一个重要的参数。如果一个节点受到网络中 t 个节点的指控, 那么认为该节点是可疑节点。 t 的取值越大, 该策略就能够抵抗越强大的恶意节点, 但同时策略的有效性也就大打折扣。反过来, 如果 t 的取值较小, 该策略就比较有效, 但更容易受到恶意攻击。因此认证的门限必须根据网络的安全需求而变化。基于门限加密机制的密钥管理服务具有较好的安全性, 它也是目前移动 Ad Hoc 网络密钥管理服务的主要研究思路。

Clique^[14] 是一种分布式的组播密钥管理算法, 通常被用来在通信双方之间协商密钥。它利用 DH(Diffie-Hellman)^[15] 密钥协商算法的一种变体来实现组密钥的生成和发布。

文献[16]中提出了将二叉逻辑密钥树应用于分布式模式的方案。文献[17]给出了另一种在分布式环境下应用二叉组播密钥树的方式, 它的密钥更新利用了 DH 算法的一种扩展形式 TGDH(Tree-based Group Diffie-Hellman)^[18]。

3 分层分组式组密钥管理策略

分层分组式的管理策略的基本思想是将参与组播的成员进行分组, 每个小组中包含一个控制节点, 所有的控制节点组成了组播密钥管理的一层, 而小组内部的密钥管理属于另一层。这两层从某种意义上是相对独立的, 它们选择的密钥管理方式可以相同, 也可以不同, 既可以是集中式, 也可以是分布式。因此, 分层分组式实际上结合了集中式和分布式的管理方式, 可以同时具备这两种方式的优点。如果小组内部的成员个数比较少, 则可以采用集中控制式; 而当小组规模比较大时, 还可以对其进行再次分组, 从而生成新的层次。

3.1 基本思想

文献[19]给出了一个采用分层分组方式的组播密钥管理策略。它的基本思想是: 所有节点的初始状态都处于最底层 L_0 ; 节点由簇生成协议分成多个簇, 每个簇通过一定的标准生成一个 leader, 称为簇头节点。 L_0 层的所有簇头节点构成 L_1 。与 L_0 一样, 在 L_1 上再次执行簇生成协议生成新的簇, 这些簇中生成的新的簇头节点再组成 L_{i+1} 。如此反复, 直到层中的成员个数为 1 时, 不再继续往上生成新的层。如图 3 所示。

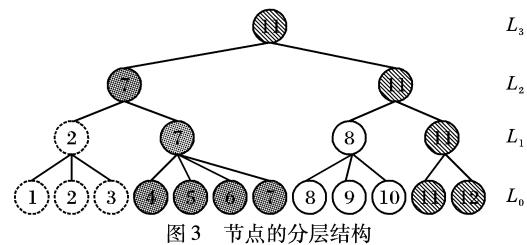


图 3 节点的分层结构

每一层有一个层密钥, 只有属于该层的成员才能知道该层的层密钥, 层密钥由密钥服务器生成。同样, 每个簇都有一个簇密钥, 只有属于该簇的成员才能知道该簇的簇密钥, 簇密钥由该簇的簇头节点生成。除此之外, 每个簇的簇头节点都

与该簇的其他成员建立点对点的安全通道。由于所有成员都属于 L_0, L_0 的层密钥被用作组密钥。层 L_i 的层密钥更新是由密钥服务器利用 L_{i+1} 层的层密钥加密, 将新的 L_i 层密钥组播发送给所有 L_{i+1} 层成员, 然后由它们利用各自在 L_i 层的簇密钥更新给所有其他的 L_i 层节点。

3.2 节点的加入与退出

在移动 Ad Hoc 网络中, 节点可能是不断移动的, 文献 [20] 初步分析了旧节点的退出和新节点的加入的几种形式。当节点退出时, 有两种情况: 如果退出节点是普通节点, 则直接将它的信息从簇头节点中删除, 同时簇头节点重新生成新的簇密钥, 分发给簇中的其他所有节点, 以保证退出的节点不能获得以后的通信信息, 即保证前向安全性; 如果退出的节点是簇头节点, 则首先要从簇中的剩余节点中根据权重选取一个新的簇头节点, 再由新的簇头节点生成新的簇密钥, 分发给所有的簇成员。

如图 3 中节点 5 退出时, 直接将节点 5 的信息从簇头节点中删除就可以了。而节点 8 退出时, 我们假设图 3 中节点 8、9、10 中, 权重从高到低依次为: 8、9、10, 因此当节点 8 退出时, 该簇中选出节点 9 作为新的簇头节点。如图 4 所示。

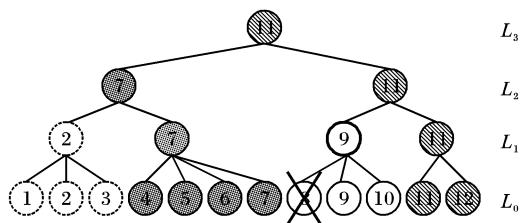


图 4 簇头节点的退出

当节点加入时, 首先将加入节点的权重与所在簇的簇头节点比较, 如果比簇头节点低, 则只需把相关信息拷贝就可以了。如果比簇头节点高, 则用新加入的节点替换原有的簇头节点, 并且将其与同一层的簇头节点比较, 重新选出上一层的簇头节点, ……, 直到新节点的权重比上一层簇头节点的权重小或替换最高层的簇头节点为止, 如图 5 所示, 加入了一个权重最大的节点 13。

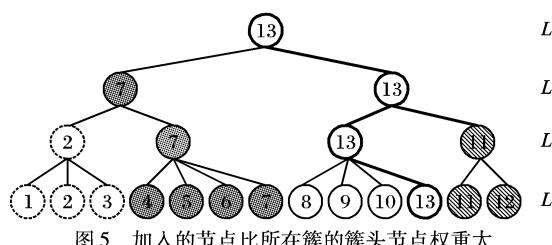


图 5 加入的节点比所在簇的簇头节点权重大

3.3 簇的分裂与合并

节点的移动与退出可能会导致网络中簇的变化。当有节点加入时, 考虑到簇头节点的负载, 可能需要对该簇进行分裂, 分裂后的多个簇需要重新产生各自的簇头节点并生成新的簇密钥; 同样, 当节点移动或退出时, 相应簇头节点的负载减小, 这时可以对网络进行优化, 从而对某些簇进行合并, 这时需要从合并的簇的多个簇头节点中选出权值最大的簇头节点充当合并后的簇的新的簇头节点, 并生成相应的簇密钥。簇的分裂与合并可以根据能量和距离等因素来决定。

Iolus^[21] 是分层分组式策略的一种具体的算法。Iolus 算法对组成员进行分组, 每个子组有一个 GSA (group security Agent: 组安全代理), 负责管理该子组, 所有 GSA 组成一个更高一级的组, 由 GSC (group security controller: 组安全控制器)

管理。它的特点是各个子组采用独立的组密钥, 组播报文在从子组 A 传播到子组 B 时要被 GSA 翻译, 即用 A 的组密钥解密, 再用 B 的组密钥加密。这种设计使得组成员关系变化所导致的密钥更新被限制在所在子组内部; 但另一方面, 组播报文的传输路径被改变了(穿越子组边界的组播报文必须经过 GSA), 而且 GSA 要负责子组的管理和组播报文的翻译, 容易成为系统的瓶颈和失效点。

4 发展方向

4.1 分析与比较

由于移动 Ad Hoc 网络自身的特殊性, 设计高效安全的组密钥管理策略难度还很大。目前密钥管理的研究主要还是针对各种特定的场合。根据移动 Ad Hoc 网络对组播密钥管理策略的需求, 对三种组播密钥管理策略的性能进行了分析和比较, 如表 1 所示。

表 1 三种策略的性能比较

	集中控制式	分布式	分层分组式
安全性	低	较高	高
同谋破解	一	较难	难
可扩展性	好	较好	较差
密钥通信代价	低	一般	高
健壮性	差	较好	好
可靠性	差	较好	好

由此可见:

(1) 集中控制式有利于组播的管理。它可以继承传统网络中各种成熟的安全协议, 还可以和主网中的其他节点实现无缝的安全连接, 特别是对于本质上使用集中控制的组播而言, 非常适合采用集中控制式的组播密钥管理。但是也容易看到, 集中式管理方式对第三方的依赖性太强, 当第三方认证服务器失效时, 将会导致认证的失败而使通信中断。而且认证服务器的性能将直接影响到系统的可扩展性, 即密钥服务器通常会成为集中控制式的瓶颈。

(2) 分布式采用的是信任分担的思想, 把权力分散在多个节点中, 这样就有效的克服了集中控制式中由于对第三方依赖性太强所带来的影响, 而且具有可扩展性, 它适用于长期的、有计划的、大型的 Ad Hoc 网络。但是分布式由于将权利分散到多个节点, 使得密钥的管理变得更加困难和复杂。

(3) 分层分组式由于结合了集中式和分布式两种方式, 所以它对某些方面的性能有所改进, 更能适应某种特殊应用, 但有些集中式或分布式所存在的问题并未从本质上加以解决。

4.2 若干研究方向

基于上面对现有移动 Ad Hoc 网络的组播密钥管理策略的分析, 我们给出该领域几个值得注意的几个方向:

(1) 对于分布式的组播而言, 由于没有中央控制节点, 各个节点间必须通过传递控制信息来维持状态的同步, 节点必须能在必要的时候主动侦测其他节点和网络的状态并采取正确的行为, 以便处理异常情况。因此, 分布式的组播密钥管理要完善密钥管理的可扩展性、健壮性和系统行为的可预测性。

(2) 组播应用因其参与节点在地域分布、性能、网络接入等情况的差异, 具有较大的多样性和复杂度, 这就要求组播密钥管理策略具有自适应、可调节能力。例如基于门限的密钥管理机制的门限必须可以根据网络状态动态优化。

(下转第 2733 页)

(mid: M_5 , mid: M_6)

由于 $C_{11} \notin C_A$, A 无法解密 M_5 , 而 $C_6 \in C_A$, 于是可以由 M_6 得到:

(mid: M_7 , mid: M_8)

由于 $C_8, C_{10} \in C_A$, B 通过解密 M_7 和 M_8 都可以得到:

end: RS

至此, A 成功的得到了资源 RS 。

隐藏证书方案的性能取决于对简单策略加密和解密函数的调用次数。考虑第 3 部分 RS 的访问策略 P_{cl} 和 P_{rs} , 原形式为 $(C_{p6} \text{ or } (C_{p8} \text{ and } C_{p11})) \text{ and } ((C_{p8} \text{ or } C_{p10}) \text{ and } C_{p7})$, 加密需要 9 次运算, 最坏情况下解密需要 9 次枚举, 而化简之后形式为 $((C_{p8} \text{ and } C_{p11}) \text{ or } ((C_{p8} \text{ or } C_{p10}) \text{ and } C_{p6})) \text{ and } C_{p7}$, 加密只需要 6 次运算, 最坏情况下解密只需要 6 次枚举。如果我们允许加密时重用中间结果, 原形式加密需要 6 次运算, 化简后加密只需要 5 次运算。由此可见, 我们的方案通过化简减少了策略中的冗余, 提高了系统效率。

如果策略无须隐藏, 可以把策略连同密文一起发送, 提高解密效率。同时, 还可以考虑把敏感资源用对称密钥加密, 而用隐藏证书根据策略来保护对称密钥, 间接地实现了对敏感

(上接第 2730 页)

(3) 设计和完善组播密钥的代价评价体系。以移动 Ad Hoc 网络的动态拓扑、时变链路、节点能量的有效性出发, 设计出一套较全面合理的代价评价体系。

(4) 将组播密钥管理对分簇的需求与现有的分簇策略^[22]进行联合优化, 使网络安全与拓扑控制机制有机结合, 以得到高效、安全的移动 Ad Hoc 网络分层体系结构。

5 结语

由于移动 Ad Hoc 网络的特殊性, 组播密钥管理策略正逐步成为该领域的研究热点。本文较全面地综述了现有的组播密钥管理策略, 对不同的策略进行了分类, 分析了各自的特点, 并给出了组播密钥管理的若干研究方向。

参考文献:

- [1] RAMANATHAN R, REDI J. A Brief Overview of Ad Hoc Networks: Challenges and Directions [J]. IEEE Communication Magazine, 2002, 23 (5): 48–53.
- [2] 叶阿勇, 许力. 移动 Ad Hoc 网络安全策略研究[J]. 微计算机应用, 2004, 25(4): 385–390.
- [3] ZHOU L, HAAS ZJ. Securing Ad Hoc Networks[J]. IEEE Networks, 1999, 13(6).
- [4] HARNEY H, MUCKENHIRN C. Group key management protocol (GKMP) specification. RFC2093[S]. 1997.
- [5] HARNEY H, MUCKENHIRN C. Group key management protocol (GKMP) architecture. RFC2094[S]. 1997.
- [6] WALLNER D, HARDER E, AGEE R. Key management for multi-cast: Issues and architectures. RFC 2627[S]. 1999.
- [7] WALDVOGEL M, GARONNI G, SUN D, et al. The VersaKey framework: Versatile group key management[J]. IEEE Journal on Selected Areas in Communications (Special Issue on Middleware), 1999, 17(9): 1614–1631.
- [8] BALENSON D, MCGREW D, SHERMAN A. Key management for large dynamic groups: One-Way function trees and amortized initialization[Z]. IETF Internet Draft (work in progress), 2000.
- [9] CANETTI R, CARAY J, ITKIS G, et al. Multicast security: A taxonomy and some efficient constructions[A]. Proceedings of the INFOCOM99[C]. New York, 1999. 708–716.
- [10] SHAMIR A. How to share a secret [M]. Communications of the ACM, 1979.
- [11] LUO H, LU S. Ubiquitous and Robust Authentication Service for Ad Hoc Wireless Network[R]. Technical Report 200030, UCLA Computer Science Department, 2000.
- [12] KONG U, ZERFOS P, et al. Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks[A]. IEEE 9th International Conference on Network Protocols (ICNP'01)[C]. 2001.
- [13] LUO H, ZERFOS P, KONG J, et al. Self-securing Ad Hoc Wireless Networks[A]. Seventh IEEE Symposium on Computers and Communications (ISCC'02)[C]. 2002.
- [14] SETINER M, TAUDIK G, WAIDNET M. Cliques: A new approach to group key agreement[R]. Technical Report, RZ 2984, IBM Research, 1997.
- [15] DIFFIE W, HELLMAN ME. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, IT-22(6): 644–654.
- [16] RODEH O, BIRMAN K, DOLEV D. Optimized group rekey for group communication systems[R]. Technical Report, Hebrew University, 1999.
- [17] LEE PPC, LUI JCS, YAU DKY. Distributed collaborative key agreement protocols for dynamic peer groups[A]. Proceedings of the ICNP[C]. 2002. 53–62.
- [18] KIM Y, PERRIG A, TSUDIK G. Simple and fault-tolerant key agreement for dynamic collaborative groups[A]. Proceedings of the 7th ACM Conference on Computer and Communications Security [C]. 2000. 235–244.
- [19] BANERJEE S, BHATTACHARJEE B. Scalable secure group communication over IP multicast[J]. JSAC Special Issue on Network Support for Group Communication, 2002, 20(8): 156–163.
- [20] 陆军, 丁雪梅. Ad-hoc 网络动态密钥管理[J]. 信息技术, 2004, 28 (7): 76–78.
- [21] MITTRA S. Iolus: A framework for scalable secure multicasting [J]. New York: ACM Press, ACM SIGCOMM Computer Communication Review, 1997, 27(4): 277–288.
- [22] 许力, 张继东, 郑宝玉, 等. 移动自组网能量保护策略研究进展 [J]. 通信学报, 2004, 25(9): 93–103.

资源的保护。

参考文献:

- [1] BALFANZ D, DURFEE G, SHANKAR N, et al. Secret Handshakes from Pairing-Based Key Agreements[A]. Proceedings of the 2003 IEEE Symposium on Security and Privacy[C]. Oakland CA, 2003. 80–196.
- [2] LI NH, DU WL, BONEH D. Oblivious Signature - Based Envelope [A]. Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing[C]. Boston Massachusetts: ACM Press, 2003. 182–189.
- [3] HOLT J, BRADSHAW R, SEAMONS K, et al. Hidden Credentials [A]. 2nd ACM Workshop on Privacy in the Electronic Society[C]. Washington DC: ACM Press, 2003. 1–8.
- [4] BONEH D, FRANKLIN M. Identity-Based Encryption from the Weil Pairing, extended abstract[A]. Proceedings of Crypto 2001, volume 2139 of Lecture Notes in Computer Science[C]. Springer-Verlag, 2001. 213–229.
- [5] BENALOH J, LEICHTER J. Generalized Secret Sharing and Monotone Functions[A]. Advances in Cryptology-CRYPTO'88, volume 403 of Lecture Notes in Computer Science[C]. Springer, 1990. 27–35.