具有自我恢复功能的密钥管理方法在 MANET 网络中应用研究

王顺满[1], 陶 然[2], 许 楷[3], 吴长奇[4]
(1. 新时代工程咨询有限公司, 北京 100088; 2. 北京理工大学电子工程系, 北京 100081
3. 电子工业出版社, 北京 100036; 4. 燕山大学信息科学与技术学院, 河北秦皇岛 066004)

摘 要: 针对 MANET 网络动态拓扑和节点处理能力弱等特征, 提出了适合 MANET 网络环境并利用密钥的上下文来恢复网络密钥的密钥管理方法, 有效地降低了系统通信量; 给出了一个安全有效的密钥分配模型, 该模型在占用内存和减少运算复杂性方面都具有非常明显的优势; 分析结果表明该方案在安全性方面具有明显优势, 分析验证了该算法在 MANET 网络中使用的有效性和可行性.

关键词: MANET; 自我恢复; 密钥管理; 自组织
中图分类号: TN 918 文献标识码: A 文章编号: 0372-2112 (2009) 04-0889-05

Research of the Self-healing Key Management in MANET

WANG Shun-man[1], TAO Ran[2], XU Kai[3], WU Chang-qi[4]
(1. *New Era Engineers Consulting Company Ltd, Beijing 100088, China;*
2. *Department of Electronics Engineering, Beijing Institute of Technology, Beijing 100081, China;*
3. *Publishing House of Electronics Engineering, Beijing 100036, China;*
4. *YanShan University, Qinhuangdao, Hebei 066004, China*)

Abstract: A self-healing key management method by using the context of the message according to the dynamic topology and low process ability of MANET is proposed in the paper, which can reduce the system communications overhead; it also offers an efficient key distribution method to reduce the memory and computation overhead compared with the common self-healing key management protocol.; the paper analyzed the research results verified the secure predominance, efficiency and availability to MANET.

Key words: MANET; Self-healing; Key management; Self-organize

1 引言

MANET 网络终端设备移动性非常强, 网络节点以自组织形式工作, 节点移动性会造成网络拓扑结构的不断变化, 网络节点有可能经常性地加入或者离开某个网络[1]. 近年来, 对 MANET 网络的安全性分析得到了越来越多人的关注, 由于 MANET 网络的动态性与自组织性, 使得传统安全措施不能在 MANET 有效使用[2,3]. MANET 的安全性除了要求保证系统的真实性、机密性和完整性之外, 还要考虑到建立可信模型和有效的密钥管理. 密钥管理是任何安全通信中必不可少的一个重要组成部分, 现有大多数密钥安全都主要依赖于固有的基础结构安全和有效的密钥分配[4]. 由于 MANET 网络的自组织性和动态性, 固定网络上常用的密钥管理手段无法在 MANET 网络中得到充分应用; 其次, 由于无线多跳网络通信的误码率比较高, 同时网络拓扑是动态变化, 会大大降低网络通信的成功率, 延长系统的服务时间; 第三, 容易导致网络拥塞, 如果网络中各节点需要到某个指定服务器上认证, 则会使本来就不宽余的网络带宽更加拥挤而造成网络拥塞.

为了保证 MANET 网络通信的安全性, 需要对通信双方的数据流进行加密, 加密过程就一定会涉及到密钥管理. MANET 安全防护特别强调前向安全性与后向安全性, 前向安全性是指新加入的网络的成员不能获取其加入以前的密钥信息, 从而不能获取加入前的信息. 后向安全性指的是被删除的网络成员不能获取其删除以后的密钥信息, 从而不能再获取删除后的信息. 因此, 当网络成员发生改变时, MANET 网络密钥需要及时更新. 由于 MANET 网络传输的不可靠可能使系统终端不能接收到更新的会话密钥而导致无法正常通信, 因此需要采取有效措施来保证更新密钥的可靠传输. 由于无线网络的动态性和不可预知性会导致网络无法正: 常通信, 又不能大量的重复传送. 因此需要找到一种实现自我恢复方法来简化服务器端的工作并降低网络通信量. 本文

收稿日期: 2005-10-18; 修回日期: 2008-01-09
基金项目: 国家自然科学基金重点项目(No. 60236010); 部委重点基金项目 (No. 6140445); 国家高校优秀青年教师教学与科研奖励计划

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

所提出的非交互自我恢复密钥管理系统的方法能保证没有正确接收到密钥的组成员可以通过正常接收的上下文信息来恢复相应密钥, 并具有较好的安全性和系统应用性能.

2 相关研究成果及存在问题

MANET 网络安全问题已经成为研究热点, 为了实现有效通信, 必须要给出有效的接入控制技术, 让经过授权的节点有权接入网络. 接入控制技术一般通过加密技术来实现, 在合法用户之间共享会话密钥. 因为 MANET 网络的动态性, 有必要通过更新密钥的方法来防范撤销用户对后续通信的访问或者让新加入用户获取以前通信内容[5,6]. 密钥管理技术可分为中心式密钥管理和协同式密钥管理两种[7], 在中心式密钥分配方法中, 中心节点(GM) 会相信一个称为 KDC 的密钥管理中心, 由 KDC 生成和分配密钥. 在协同式密钥管理方法中, 组成员具有同等的信任关系, 他们共同参与到组密钥的管理工作中. 不论中心式密钥管理还是协同式密钥管理都能够对动态成员变化的接入和减少计算量、通信量和终端的存储量为目标.

Zhou 和 Hass 在文献[8] 中给出了一中基于(n, k)门限思想的安全密钥分配方法, 这种方案能够抵挡最大 $k-1$ 个终端设备的协同攻击. 然而, 该系统并没有给出服务器在整个网络中随机分布时如何实现终端设备与服务器的安全连接. 在该方案中还提出了抵御移动破坏节点的共享更新方法, 然而, 对如何实现安全有效的密钥分配却没有给出确切说明. Yi, Naldurg 和 Kravets 在文献[9] 中给出了一种称为 MOCA 的密钥管理方案. 在这种方法中, 证书服务被具有移动证书授权(MOCA) 功能的网络节点所完成, 这些充当 CA 功能的网络节点比其它节点具有更高的安全性. 在这个系统中, 1 个网络节点能够同时被 $k+\alpha$ 个 MOCA 节点来定位, 整个定位过程或者是通过最短路径或者是基于路由以随机方式实现. 但是, 最重要的问题是这些网络节点如何来安全地发现这些路径, 因为大多数安全路由协议都是基于已经建立的密钥服务基础之上. Luo, Kong 和 Zerfos 在文献[10] 中提出了一种称为 URSA 的局部密钥管理方案. 在该系统中, 所有的节点都是服务器. 其优点是在能够保证系统可用性的情况下还能够有效地实现安全本地通信, 另外, 这种方法在系统终端没有得到安全保护的时候会降低系统的整体安全. 该系统的另一个问题是当门限值 k 比网络层数 d 大得多时, 网络终端将不得不通过不断移动来获取更新后的密钥; 第二个问题是共享密钥更新过程的聚合问题; 第三个问题是在接入网络之前要求大量的预先配置. Capkun, Buttyan 和 Hubaux 在文献[11] 中给出了一种完全分布式的解决方案, 该方案的明显优势在于配置过程非常灵活. 然而, 在信任结构中缺少任何可信的安全端点, 并需要生成许多证书. 每个节点都需要搜集并维护一个实时更新的证书库; 证书链被用来实现对公钥的认证; 证书图被用来映射网络信任关系, 这个图要求具有强连接性, 在 MANET 网络中对其有特别地要求. 在 MANET 网络中, 在一个区域中的网络节点可能不会与其它范围的网络节点进行通信, 但是在这个系统中容易造成证书冲突, 因此需要引入一个能够提高证书存储量的方案. Yi 和 Kravets 等人在文献[12] 给出了一种组合的信任模型, 在给出的方案中, 将中心信任模型和完全分布式的信任模型结合起来, 利用两种不同信任模型的优点, 事实上, 这种方案在安全性要求和灵活性要求之间进行了折中. 然而, 对信任值的指定和分配是该系统的一个重要问题. Canetti 和 Garay 等在文献[13, 14] 中给出了动态组用户的密钥更新机制, 并在文献[1517] 给出了对非法用户的跟踪功能. 所有这些文献都假定网络自身是安全的. Wallner 和 Stinson 等在文献[18] 和文献[19] 对 MANET 网络中数据传输失效的问题进行了分析, 首先在 MANET 网络中引入了差错控制功能, 另外需要在数据包的后面附加一些提示信息来使系统具有自我恢复功能. Staddon 等人在文献[20] 中对数据包传输过程中的丢失问题进行了分析, 每个数据包都能够让用户恢复出当前密钥以及前面和后面的共享密钥.

本文根据文献[21] 给出的具有自我恢复能力密钥系统的思想, 提出实现自我恢复功能的密钥管理体制, 同时给出一种安全和有效的自我恢复密钥管理系统结构. 文献[21] 指出, 在两个广播消息 B_{j_1} 和 B_{j_2} 中的某个用户能够恢复出所有属于 $j_1 \leqslant j \leqslant j_2$ 的密钥 K_j, 但是该方案却没有给出对 $K_1, \cdots, K_{j-1}$ 的说明, 也没有给出密钥恢复的具体方法. 本文所设计的方法能够有效地从 B_{j_1} 和 B_{j_2} 中恢复出任何满足 $j \leqslant j_2$ 条件的密钥 K_j, 同时在性能上和安全性方面都具有非常明显的优势.

3 具有自我恢复功能密钥管理方案

为使系统具有抵抗协同攻击的能力, 在一个给定系统中, 不同用户恢复出的共享密钥是不同的. 密钥分配系统抵抗协同攻击的能力与每个阶段由用户恢复出的共享密钥之间的依赖程度有关, 可以通过使用高阶多项式来提供系统抵抗协同攻击能力. 在这里给出了一个具有自我恢复功能和撤销能力的密钥分配系统.

3.1 GM 的生成

首先采用基于门限思想的方法来生成 GM, 每次密钥的生成和管理过程中, 要在 n 个用户中选择 k 个作

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

为被选用户, 由他们协同起来实施对 MANET 网络的管理. 这样做的好处在于能够让系统有效防范系统的单点失效, 使系统的管理任务并不仅仅依赖于某一个节点.

3.2　系统建立

假定 t 为一个正整数, N 为域 F_q 中与任何用户索引值不同的一个元素. GM 要在域 F_q 中选择 m 个多项式 $p_1(x), p_2(x), \cdots, p_m(x)$, 这些多项式都是 t 阶的, 域 F_q 中的 m 个会话密钥 $K_1, \cdots, K_m$ 都是随意选择的, 对每个 $j=1, \cdots, m$ 都定义了一个对应的多项式 $q_j(x)=K_j-p_j(x)$. 对于 $j=\{1, \cdots, m\}$ 来讲, GM 要对 $i=1, \cdots, m$ 在 $F_q[x, y]$ 中选择 m 个多项式 $s_{1,j}, s_{2,j}, \cdots, s_{m,j}$. 其中, $s_{(i,j)}(x, y)=a_{0,0}^{i,j}+a_{1,0}^{i,j}x+a_{0,1}^{i,j}y+\cdots+a_{t,t}^{i,j}x^t y^t$ 同时, 对任何一个属于 $i\in(1, 2, \cdots, n)$ 的用户 U_i 来讲, 存储对应的私钥.

$$S_i=\{N, i, s_{1,1}(i, i), \cdots, s_{m,1}(i, i), s_{1,2}(i, i), \cdots, s_{m,2}(i, i), \cdots, s_{1,m}(i, i), \cdots, s_{m,m}(i, i)\}$$

3.3　广播

假定 $A, R\subseteq\{U_1, \cdots, U_n\}$, 满足 $|R|\leqslant t$ 的条件, 这里的 A 和 R 分别代表在会话 j 中的有效用户和撤销用户. GM 选择 $W=\{w_1, w_2, \cdots, w_t\}\subseteq F_q$, 满足将 R 中的用户索引能够包含在 W 中, 而 A 中的用户索引不会包含在 W 中, 并且 $N\notin W$. 在周期 $j\in\{1, \cdots, m\}$ 中的广播消息为 $B_j^1\cup B_j^2$. 这里的 B_j^1 和 B_j^2 分别为:

$$B_j^1=\{p_{j'}(x)+s_{j',j}(N, x)\}_{j'=1, \cdots, j-1}\cup\{K_j+s_{j,j}(N, x)\}\cup\{q_{j'}(x)+s_{j',j}(N, x)\}_{j'=j+1, \cdots, m} \quad (1)$$

$$B_j^2=\{W_l, \{s_{j',j}(w_l, x)\}_{j'=1, \cdots, m}\}_{l=1, \cdots, t} \quad (2)$$

3.4　密钥恢复

对所有 $i\in(1, \cdots, n)$ 来讲, U_i 都能够通过在 $x=i$ 处计算多项式 $\{s_{j,j}(w_l, x)\}_{l=1, 2, \cdots, t}$ 并通过对点 $(i, s_{j,j}(i, i))$ 和 $\{(w_l, s_{j,j}(w_l, i))\}_{l=1, 2, \cdots, t}$ 的插值操作来恢复 $s_{j,j}(x, i)$. 然后, U_i 对在 $x=N$ 处计算得到的 $s_{j,j}(x, i)$ 减去 $(K_j+s_{j,j}(N, x))|_{x=i}$ 的值来恢复会话密钥 K_j. 另外, U_i 能够通过插值方法来决定 $\{s_{j',j}(x, i)\}_{j'=1, 2, \cdots, j-1, j+1, \cdots, m}$ 并恢复共享密钥 $\{P_{j'}(i)\}_{j'=1, 2, \cdots, j-1}$. 通过同样的方法可以恢复 $\{q_{j'}(i)\}_{j'=j+1, j+2, \cdots, m}$.

3.5　密钥分配

U_i 按照上面给出的方法来恢复密钥 K_j 和其它共享密钥. 同时随机地将 $z_{i,j}=\{p_1(i), \cdots, p_{j-1}(i), K_j, q_{j+1}(i), \cdots, q_m(i)\}$ 发送给域 F_q 子集中仅仅拥有广播消息或者个人密钥的用户. 另外, 对仅有 t 个用户的集合来讲, 当 $j'\in\{1, 2, \cdots, m\}$ 时, 对于满足 $U_i\notin B$, $i\notin W$ 的用户 B 是不能决定 $s_{j',j}(i, i)$ 的. 因为它仅仅能够在 $x=i'\in W(i\notin w)$ 恢复出多项式 $s_{j',j}(x, i)$ 上的点以及 $x=i'$ 和 $U_i'\in B$ 时多项式 $s_{j',j}(i, x)$ 上的点. 因此, 给定每个多项式的阶数 t 之后, $s_{j',j}(i, i)$ 仍然能够在域 F_q 中向 B 中的用户随机地分配. 因为在 $s_{j',j}(*, *)$ 中没有任何关于 $j'\in\{1, 2, \cdots, m\}$ 的信息, 所以, 接下来要发送的消息为: $H(s_{j',j}(i, i))|\{S_i\}\, i\in B, B_1, B_2, \cdots, B_m=H(S_{j',j}(i, i))$.

3.6　密钥撤销

在广播信息

$\cup_{U_i\in R, z_{i',j}}=\{s_{j',j}(i', x)\colon U_i'\in R, j'=1, 2, \cdots, m\}$ 中如何获得 t 个撤销用户的 R 信息. 对于 $i=1, 2, \cdots, n$ 来讲, 撤销用户能够知道多项式 $\{s_{j',j}(x, i)\}$ 中的至少 t 个点, 且代表撤销用户的每个点 $\{s_{j',j}(N, i)\}$ 在域 F_q 中是任意分配的. 因为对 $j=1, 2, \cdots, m$ 和所有的 i 来讲, 撤销用户没有关于 $\{s_{j',j}(N, i)\}$ 的消息, 因此撤销用户就没有任何关于 $\{s_{j',j}(N, x)\}$ 的信息. K_i 的计算式为:

$$H(K_j|B_j, \{S_i'\}U_i'\in B)=H(K_j) \quad (3)$$

3.7　自我恢复

对于 $j_1<j<j_2$ 来讲, 用户 U_i 通过 B_{j_1} 来获取 $q_j(i)$, 通过 B_{j_2} 来获取 $p_j(i)$. 因此 $K_j=P_j(i)+q_j(i)$ 能够通过 B_{j1} 和 B_{j2} 来重建. 这里用 G 来表示群用户, 他们都属于在 $j_2>j$ 时 j 个会话中被撤销和在 $j_1<j$ 的会话时的有效用户. 用 C 表示满足 $j_1<j$ 时第 j 个会话中被撤销群用户以及 $j_2>j$ 时的有效用户. 这里的 G 和 C 互不连接, 并且 $|G\cup C|\leqslant t$, 那么在 $G\cup C$ 中的协同用户是不能在广播信息中 B_{j_1} 和 B_{j_2} 中恢复出密钥 K_j 的. 为了恢复 K_j, $G\cup C$ 要在 B_{j_1} 中恢复 $q_j(i)$, 在 B_{j_2} 中恢复 $p_j(i)$. 因为在 C 中的用户在会话 j_1 中被撤销, 所以 $G\cup C$ 仅仅能够用来恢复 $\{q_j(i)\}_{U_i\in B}$, 同时在 B 中的用户在会话 j_2 中撤销的, 所以 $G\cup C$ 仅仅能够恢复出 $\{p_j(i')\}_{U_i'\in C}$. 因为 G 和 C 相互不连接, B 和 C 的最大规模都为 t, $p_j(x)$ 和 $q_j(x)$ 的最佳阶数也都为 t, 因此通过这些信息不能恢复出 K_j.

4　系统实现与性能分析

这里用 GM 表示组管理者, 用 $U_1, U_2, \cdots, U_n$ 来代表 n 个网络用户, 每个用户 U_i 都要存储一个私钥 S_i, 这个私钥可以看作是有限域 F_q 元素中的子集, 这里要求 $q>n$, 私钥可以是相关的. 所有操作都是在有限域 F_q 中实现的, 对于 $j=1, 2, \cdots, m$ 来讲, 会话密钥 K_j 会在 GM 通过 B_j 以广播方式发送到各终端用户. 对于属于组 G 中的用户 U_i 来讲, 对应的会话密钥 K_j 由 B_j 和 S_i 共同决定.

4.1　系统操作过程

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

每个组用户在接收到广播 B_j 消息以后, 通过它的私钥计算会话密钥 K_j, 会话密钥 K_j 的生成是以相同的概率由 *GM* 生成. 由来 S_i, B_j, K_j 表示与上述元素有关的随机变量, 并用熵函数来严格地表述具有自我恢复功能的密钥分配系统. 事实上, 通过熵函数能够更加清晰地描述该协议.

假定 $i\in\{1, 2, \cdots, n\}$, $j\in\{1, 2, \cdots, n\}$, 在满足如下 2 个条件之后 D 就为具有自我恢复功能的会话密钥分配系统.

1, 对于 $U_i\in G$ 来讲, 会话密钥 K_j 由 S_i 和 B_j 共同决定, 用公式表示为:

$$H(K_j|S_i, B_j)=0 \tag{4}$$

2, 对任何 $j=1, 2, \cdots, m$ 来讲, 用户 $U_1, U_2, \cdots, U_n$ 都不仅仅通过广播消息或者私钥来获得与会话密钥 K_j 有关的任何信息. 用公式表示为:

$$H(K_j|B_1, \cdots, B_m)=H(K_j|S_1, \cdots, S_n)=H(K_j) \tag{5}$$

条件 1 和条件 2 说明对于 G 中的每个用户来讲, 通过广播消息和它自己的私钥能够恢复出对应的会话密钥, 但是, 当仅仅给出广播消息或者用户私钥的话是不能获得任何与会话密钥有关的消息.

4.2 系统安全性分析

4.2.1 独立于以后的会话密钥

对所有的 $U_i\in G$ 来讲, 在 $j=m-r+1, \cdots, m$ 时, 如果不广播 B_j, 就不能计算出任何与密钥 $K_{m-r+1}, \cdots, K_m$ 有关的消息. 用公式来表示为:

$$H(K_{m-r+1}, \cdots, K_m|S_1, S_2, \cdots, S_m, B_1, B_2, \cdots, B_{m-r})=H(K_{m-r+1}, \cdots, K_m) \tag{6}$$

上述条件说明, 后续的广播消息对恢复会话密钥是必须的.

4.2.2 抗协同攻击能力

对于满足 $|F|\leqslant t$ 和 $U_i\notin F$ 条件的任何子集 $F=\{U_{l_1}, \cdots, U_{l_f}\}\subseteq\{U_1, \cdots, U_n\}$ 来讲, 在 F 中的用户不能得到任何与 S_i 有关的消息. 用公式表示为:

$$H(S_i|S_F, B_1, \cdots, B_m)=H(S_i) \tag{7}$$

其中, S_F 表示 $S_{l_1}, S_{l_2}, \cdots, S_{l_f}$ 上述条件能够建立一个具有抵抗 t 个用户协同攻击能力的密钥分配系统.

4.2.3 自我恢复能力

对 $U_i\in G$ 的每个用户来讲, 当 $1\leqslant r<s\leqslant m$ 时, 在广播消息 B_r 和 B_s 中都能恢复出的 $j=r, \cdots s$ 所有 K_j. 用公式表示为:

$$H(K_r, \cdots, K_s|S_i, B_r, B_s)=0 \tag{8}$$

上述条件对自我恢复系统进行了说明: 任何两个广播消息都足够来恢复出在会话 r 和会话 s 中的所有的会话密钥.

4.2.4 用户撤销

在 $|R|\leqslant t$ 时, 给定任何 $R=\{U_{l_1}, \cdots, U_{l_r}\}\subseteq\{U_1, \cdots, U_m\}$ 子集. *GM* 都能够生成广播消息 B_j. 对任何 $U_i\notin R$ 来讲, 用户 U_i 能够恢复出密钥 K_j 但是撤销用户却不能. 用公式表示为:

$$H(K_j|B_j, S_R)=H(K_j) \tag{9}$$

这里的 S_R 代表 $S_{l_1}, S_{l_2}, \cdots, S_{l_r}$ 上述条件所考虑的是用户撤销行为, *GM* 能够撤销组中的任何成员.

4.2.5 前向与后向安全性

让 g_1 和 g_2 表示两个整数, 并且 $g_1+g_2=t$. 规模为 g_1 的一组用户 $G_1=\{U_{l_1}, \cdots, U_{l_{g1}}\}$ 在会话 j_1 之前被移除, 规模为 g_2 的一组用户 $G_2=\{U_{P_1}, \cdots, U_{P_{g2}}\}$ 在会话 j_2 之后加入到组中, 这两个组都不能获得任何与密钥 K_j 有关的信息. 对 $j_1<j<j_2$ 来讲, 用公式表示为:

$$H(K_j|B_1, \cdots, B_m S_{G_1}, S_{G_2})=H(K_j) \tag{10}$$

这里的 S_{G_1} 代表 $S_{l_1}, \cdots, S_{l_{g1}}$, S_{G_2} 表示 $S_{P_1}, \cdots, S_{P_{g2}}$, 上述条件说明, 这个系统能够有效地防范协同攻击, 并在撤销用户和新接入用户组成的群中实现前向和后向安全性.

4.3 系统性能分析

Hanaoka 在文献[21]给出的方案中, 广播包的大小为: $|B_j|=mt\log q+mt^2\log q$, 私钥长度为 $S_i|=m^2$. 在我们所设计的结构中, 终端用户存储的个人私钥 S_i 长度为 $|S_i|=m$, 同时, 广播包的大小为 $|B_j|=jt\log q+jt^2\log q$. 因此相比较 Hanaoka 方案来讲, 系统在性能方面具有非常明显的提高.

4.4 该方案相比 **Hanaoka** 方案具有的优势

给定自我恢复功能方案与 Hanaoka 方案在实现方法上的不同. 在 Hanaoka 方案中, 任何用户都可以在广播消息 B_{j_1} 和 B_{j_2} 之间恢复出属于 $j_1\leqslant j\leqslant j_2$ 之间的密钥 K_j. 给定方法可以将其扩展到通过广播消息 B_{j_1} 和 B_{j_2} 来恢复所有满足 $j\leqslant j_2$ 的会话密钥 K_j. Hanaoka 方案满足 $U_i\in G$ 对于任何满足的用户来讲, 通过一个广播消息 B_j 仅仅能够恢复出 K_j 的条件. 用公式来表示为:

$$H(K_1, \cdots, K_{j-1}, K_j, K_{j+1}, \cdots, K_m|S_i, B_j)=H(K_1, \cdots, K_{j-1}, K_j, K_{j+1}, \cdots, K_m) \tag{11}$$

给定方案并不需要满足这个强制条件, 因为一个授权用户能够通过广播消息 B_j 得到属于群组中的其它部分密钥信息, 对这个条件的放宽不会影响到整个系统的安全性. 上述协议可以让 *GM* 与用户一起对 m 个不同的会话建立会话密钥, 通过使用 F_q^* 中的公钥生成因子 g, 将所有计算都变成指数计算, 本协议能够建立一个计算安全的长效协议, 在这里就不对指数运算的安全性给出过多的分析.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

5 结论

本文给出了一个能够减少 MANET 网络流量和网络管理节点系统负荷并能够有效防范流量分析攻击具有自我恢复功能的密钥分配体制. 该方案相比 Hanaoka 的方案具有更强的自我恢复功能并降低了约束条件. 同时, 该方案在占用内存和减少运算复杂性方面具有非常明显优势. 由于本方案在实现过程中需要额外的控制功能会增加数据包的规模, 因此下一步的工作是找到既能实现自我恢复, 又能较少数据包规模更为有效的方法.

参考文献:

[1] V Karpijoki. Security in ad hoc networks [A]. Tik-110. 501 Seminar on Network Security [C]. HUT TML, 2000.

[2] S Marti, T Giuli, K Lai, M Baker. Mitigating routing misbehaviour in mobile ad-hoc networks [A]. Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking [C]. New York, NY, USA: ACM, 2000. 255–265.

[3] H Luo, S Lu. Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks [R]. Technical report UCLA-CSD-TR-200030, October 2000.

[4] Y Kim, A Perrig, G Tsudik. Simple and fault-tolerant key agreement for dynamic collaborative groups [A]. S Jajodin, P Samarati (eds). Proceedings of the 7th ACM Conference on Computer and Communications Security [C]. New York: ACM, 2000, 235– 241.

[5] M J Moyer, J R Rao, P Rohatgi. A survey of securely issues in multicast compunctions[J]. IEEE Network, 1999, 13(6): 12– 23.

[6] RFC 2627, Key Management for Multicast: Issues and Architectures [S]. Internet Draft Report. Sept. 1998.

[7] R Canetti, J Garay, G Itkis, D Miccianancio, M Naor, K Pinkas. Multicast security: a taxonomy and some efficient constructions [A]. Proceedings of Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies [C]. 1999, vol. 2, 708– 716.

[8] Zhou L, Z Haas. Securing ad hoc networks [J]. IEEE Network Magazine, 1999, 13(6): 24– 30.

[9] S Yi, P Naldurg, R Kravets. Security-aware ad-hoc routing for wireless networks [A]. Proceedings of the Symposium on Mobile Ad Hoc Networking and Computing [C]. ACM, 2001, 299 – 302.

[10] H Luo, S Lu. URSA: Ubiquitous and robust access control for mobile ad-hoc networks [J]. IEEE-ACM Transactions on Networking, 2004, 12(6): 1049– 1063.

[11] S Capkun, L Buttyan, J Hubaux. Self-organized public-key management for mobile ad hoc networks [J]. IEEE Transactions on Mobile Computing, 2003, 2(1): 52– 64.

[12] S Yi, R Kravets. Composite key management for ad hoc networks [A]. Proceedings of First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04) [C]. IEEE Press, 2004, 52– 61.

[13] R Canetti, J Garay, G Itkis, D Micciancio, M Naor, B Pinkas. Multicast security: a taxonomy and some efficient constructions [J]. Proceedings of Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies [C]. IEEE Press, vol. 2, 1999, 708– 716.

[14] R Canetti, T Malkin, K Nissim. Efficient communication-storage tradeoffs for multicast encryption [A]. Advances in Cryptology- Eurocrypt'99 [C]. Springer Berlin/Heidelberg, vol. 1592, 1999, 459– 474.

[15] B Chor, A Fiat, M Naor, B Pinkas. Traitor tracing [J]. IEEE Transactions on Information Theory, 2000, 46(3): 893– 910.

[16] A Fiat, T Tessa. Dynamic traitor tracing [J]. Journal of Cryptology, 2001, 14: 211– 223.

[17] J N Staddon, D R Stinson, R Wei. Combinatorial properties of frameproof and traceability codes [J]. IEEE Transactions on Information Theory, 2001, 47(3): 1042– 1049.

[18] RFC2627, Key Management for Multicast: Issues and Architectures [S].

[19] D R Stinson, R Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes[J]. SIAM Journal on Discrete Mathematics, 1998, 11(1): 41– 53.

[20] J Staddon, S Miner, M Franklin, D Balfanz, M Malkin, D Dean. Self-healing key distribution with revocation [A]. Proceedings of the 2002 IEEE Symposium on Security and Privacy [C]. Washington, DC, USA: IEEE Computer Society, 2002. 12– 15.

[21] G Hanaoka, T Nishioka, Y Zheng, H Imai. An efficient hierarchichal identity-based key-sharing method resistant against collusion-attacks [A]. In Advances in Cryptology-Asiacrypt'99[C]. Springer-Verlag, London, UK, 1999, 348– 362.

作者简介:

王顺满　男, 出生于黑龙江省齐齐哈尔市, 高级工程师. 现工作于新时代工程咨询有限公司, 主要研究方向为信息系统与信息安全. 发表学术论文 30 余篇, 出版著作 3 部, 申请国家专利 5 项, 3 次获部级科技进步奖.

陶　然　男, 出生于安徽, 教授, 博士生导师, 现工作在北京理工大学. 主要研究方向为信息系统与信息对抗. 发表学术论文 100 余篇, 获国家杰出青年等荣誉称号.

许　楷　女, 出生于河北省秦皇岛市, 编辑, 现为电子工业出版社团委书记. 主要研究方向为信息系统与通信系统. 发表学术论文 10 余篇, 多次获部级奖励.

吴长奇　男, 出生于黑龙江省齐齐哈尔市, 教授, 现工作在燕山大学信息科学与工程学院. 主要研究方向为移动通信与信号处理. 发表学术论文 40 余篇, 出版著作 2 部.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net