适用于传感器网络的分级群组密钥管理

李凤华[1,2], 王 巍[1,3], 马建峰[1]
(1. 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, 陕西西安 710071;
2. 北京电子科技学院研究生处, 北京 100070;
3. 中国电子科技集团公司第三十六研究所, 浙江嘉兴 314033)

摘 要: 由于无线传感器网络中经常出现节点加入或离开网络的情况, 所以需要建立一种安全高效的群组密钥管理系统来保证无线传感器网络中群组通信的安全性. 提出了一种基于密钥树和中国剩余定理的分级群组密钥管理方案. 有 sensor 节点加入, 先向新成员发送二级群组密钥, 可参与一些不太敏感的数据的传送; 待新成员获得 GCKS 的信任之后, 则向其发送群组密钥, 从而可参与有关机密信息的会话. 节点离开时, 通过利用完全子集方法将剩余成员进行分割, 提出的方案可以利用中国剩余定理对群组密钥进行安全的更新. 证明方案满足正确性、群组密钥保密性、前向保密性和后向保密性等安全性质. 性能分析表明, 此方案适合应用于无线传感器网络环境.

关键词: 群组密钥管理; 无线传感器网络; 中国剩余定理; 密钥树
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2008) 12-2405-07

Leveled Group Key Management for Wireless Sensor Networks

LI Feng-hua[1,2], WANG Wei[1,3], MA Jian-feng[1]
(1. *Key Laboratory of Computer Networks and Information Security (Ministry of Education), Xidian University, Xi'an, Shaanxi 710071, China;*
2. *Graduate School, Beijing Electronic Science and Technology Institute, Beijing 100070, China;*
3. *No. 36 Research Institute of CETC, Jiaxing, Zhejiang 314033, China*)

Abstract: Since the sensor nodes join or leave the wireless sensor networks (WSNs) frequently, it is necessary to build a secure and efficient group key management system. Based on the key tree and the Chinese remainder theorem, a leveled group key management scheme is proposed. The new sensor may transmit some not sensitive messages by the sublevel group key sent to it, and a group key is sent to the new sensor so as to let it join the WSN in deed after it gets the trust of GCKS. In the leave event, the remaining nodes in the key tree are partitioned by the complete subset method. Then the group key can be updated securely by the method based on Chinese remainder theorem. Finally, we show that the proposed scheme satisfies the desired security properties, such as correctness, group key secrecy, forward secrecy and backward secrecy. The performance analysis shows that the proposed scheme is be applicable to WSNs.

Key words: group key management; wireless sensor networks; Chinese remainder theorem; key tree

1 引言

无线传感器网络(WSNs, Wireless Sensor Networks)中安全的群组通信需要所有授权传感器节点共享一个群组密钥. 信息的发送者通过群组密钥对群组通信的内容进行加密后把加密结果发送到网络. 但是, 由于 WSNs 中经常会发生传感器节点的加入和离开事件, 如需要通过增加传感器节点监测更广泛的范围、传感器节点发生错误与网络断开、传感器节点遇到入侵需要从网络中隔离出去、传感器节点受到信号干扰不能与其他节点相连、运动的传感器节点短暂移出/移入侦测范围、传感器节点电量不足或短暂临时处于维修状态等, 这时需要更新群组密钥, 使得离开的传感器节点不能访问当前及以后的通信内容, 而新加入的传感器节点也不能访问其加入前的通信内容, 从而保证群组通信的安全性. 同时, 由于新传感器节点加入网络后只能得到群组控制者和密钥服务器(GCKS, Group Controller and Key Server)的部分信任, 需要经过一段时间后此节点才能得到 GCKS 的完

收稿日期: 2008-07-23; 修回日期: 2008-08-15
基金项目: 国家 863 高技术研究发展计划(No. 2007AA01Z429, No. 2007AA01Z472, No. 2007AA01Z482); 国家自然科学基金(No. 60633020, No. 60573036, No. 60702059); 北京市自然科学基金(No. 4082028); 陕西省"13115"科技创新工程重大科技专项(No. 2007ZDKG-56)

全信任,所以用一个群组密钥不能满足这种情况,需要设计一种高效的分级群组密钥管理方案来解决 WSNs 中的安全群组通信问题.

文献[1~3]提出了基于密钥树结构的适用于 WSNs 的群组密钥管理方案,但这些方案的性能受限于密钥树结构. 文献[4]提出了一种使用组合数学理论对群组密钥进行管理的方案 EBS(Exclusion Basis Systems). 文献[5]提出了基于 EBS 和 t 次二元多项式的群组密钥管理方案. 但文献[4,5]没有考虑 EBS 容易受到共谋攻击的问题. 文献[6,7]提出了基于 EBS 的分布式密钥管理方案来抵抗共谋攻击,但并没有考虑当前会话中群组成员共谋的情况. 文献[8]针对 EBS 容易受到共谋攻击的问题,给出了一个基于传感器节点位置和 EBS 系统的群组密钥管理方案 SHELL(Scalable, Hierarchical, Efficient, Locatiorr aware, and Light-weight Sheme). SHELL 通过增加共谋链的长度来解决 WSNs 中攻击者通过少量共谋节点获得所有的管理密钥从而导致网络被捕获的问题. 但 SHELL 存在以下缺点:使用多个 EBS 系统、为节点分配密钥组合时采用广度优先的顺序、只考虑了两个节点间海明距离尽量小的问题、采用的启发式密钥组合分配方法容易导致 NP 问题等.

本文提出了一种针对传感器网络的基于密钥树和中国剩余定理的分级群组密钥管理方案,给出了相应的系统建立、节点加入和节点离开的处理方法,并在节点加入时将群组密钥分为两级:先分配二级群组密钥,可以让新成员参与一些不太敏感的数据的传送,若一段时期之后新成员获得 GCKS 的信任,则向其发送群组密钥. 这样可以很好地解决上述提到的问题. 最后对设计的群组密钥分发方案的安全性和性能进行了分析.

2 基于密钥树和中国剩余定理的分级群组密钥管理方案

2.1 系统建立

设无线传感器网络的规模为 N(网络中的节点数量). GCKS 构造并维护一棵和 sensor 节点对应的二叉密钥树 T. 在 T 中,每个节点用标号$<l, v>$表示,这里 l 表示此节点的层数,v 表示此节点是 l 层的第 v 个节点. 由于第 l 层至多有 2^l 个节点,所以有 $0 \leqslant v \leqslant 2^l - 1$. T 的每个叶子节点对应无线传感器网络中的一个 sensor 节点. 图 1 给出了一个密钥树的例子.

GCKS 选择一个充分大的正整数 p,为 T 的每个节点$<l, v>$选择一个与其他节点不同的节点密钥 $k_{<l,v>}$ 满足 $k_{<l,v>} > p$. 这里要求 T 的所有节点密钥两两互素. 对于每个 sensor 节点,T 中从该 sensor 节点对应的叶节点到根节点路径上的 l 个节点称为此 sensor 节点的密钥路径,对应的节点密钥称为该 sensor 节点的密钥组. 在图 1 中,sensor 节点 u_2 的密钥组为:$\{k_{<0,0>}, k_{<1,0>}, k_{<2,0>}, k_{<3,0>}, k_{<4,1>}\}$. GCKS 通过安全的方式将每个 sensor 节点的密钥组中的密钥分发给相应的 sensor 节点. 在 T 中,节点$<l, v>$的节点密钥 $k_{<l,v>}$ 由以该节点为根的子树的叶子节点对应的 sensor 节点共同拥有. 如图 1 中,节点$<2, 1>$的节点密钥 $k_{<2,1>}$ 由 sensor 节点 u_5、u_6、u_7、u_8 共同拥有. 特别地,根节点的节点密钥 $k_{<0,0>}$ 由所有 sensor 节点共同拥有,每个叶子节点的节点密钥由对应的 sensor 节点单独拥有,记 sensor 节点 u_i 拥有的叶子节点的节点密钥为 k_{u_i}.

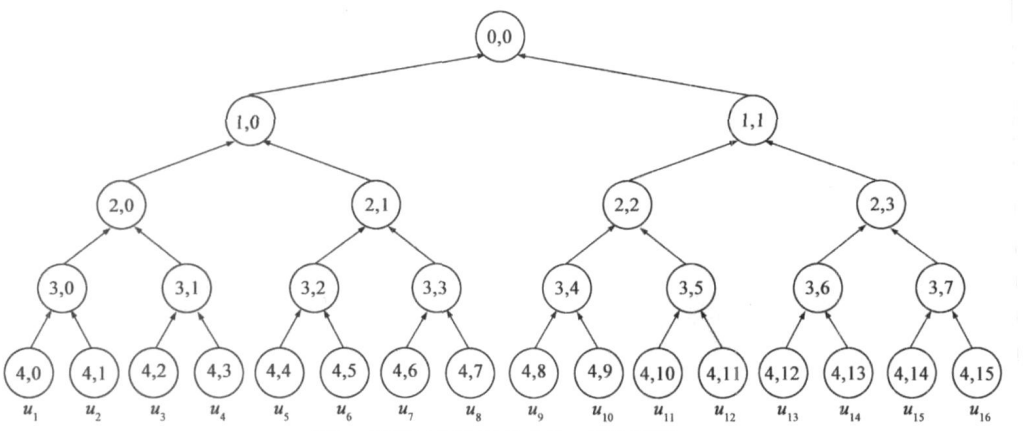


图1 具有16个叶子节点的二叉密钥树

下面利用类似文献[9]中的方法构建群组密钥. 假设无线传感器网络中有 N 个 sensor 节点,GCKS 利用这些 sensor 节点的密钥 k_{u_1}、k_{u_2}、…、k_{u_N} 计算:$M = k_{u_1} k_{u_2} \cdots k_{u_N}$,$M_i = M / k_{u_i}$ 和 M_i 在模 k_{u_i} 下的乘法逆元 M_i',即满足 $M_i M_i' \equiv 1 (\mathrm{mod}\ k_{u_i})$,$i = 1 \sim N$. GCKS 在小于 p 的正整数中随机选择群组密钥 K,$0 < K < p$. 利用 sensor 节点的密钥 k_{u_1}、k_{u_2}、…、k_{u_N} 和群组密钥 K 计算 N 个数 $n_1, n_2, \cdots, n_N$,其中 $n_i = k_{u_i} - K$,$i = 1 \sim N$. 根据 sensor 节点的密钥和群组密钥的选取可知 $0 < n_i < k_{u_i}$. GCKS 利用整数 k_{u_i}、n_i、M、M_i 和 M_i'($i = 1 \sim N$)计算中国剩余定理的唯一解

$X=(\sum_{i=1}^{N}n_iM_iM_i')\bmod M$, 并通过群组密钥分发消息将解 X 发送到无线传感器网络中. 这时, 群组密钥 K 被隐藏在解 X 中.

sensor 节点 u_i 收到群组密钥分发消息后, 利用其密钥 k_{u_i} 和中国剩余定理的解 X 通过 1 次取模运算和 1 次减法运算计算出群组密钥 K: $K=k_{u_i}-(X \bmod k_{u_i})$.

在上述群组密钥分发方案中, 只有合法的 sensor 节点才能利用其密钥正确计算出群组密钥 K, 而其他非授权 sensor 节点即使获得 X 也不能计算出群组密钥. 因而, 该群组密钥分发方案可以实现对 sensor 节点的自动授权. 同时, sensor 节点拥有的密钥保持不变, 避免了 sensor 节点密钥的更新过程.

2.2 sensor 节点加入事件

假设无线传感器网络中有 N 个 sensor 节点 $\{u_1, \cdots, u_N\}$, 希望加入网络的 sensor 节点为 u_{N+1}, 其节点密钥为 $k_{u_{N+1}}$. 在我们的方案中, 使用了两种群组密钥: 群组密钥 K 和二级群组密钥 K'. 其中 K 的作用和传统的群组密钥相同, 而 K' 用来分配给刚加入群组的 sensor 节点. 同时, 拥有 K 的节点可以推导出 K'. 在通信时 GCKS 和 sensor 节点使用 K 加密机密数据, 使用 K' 加密机密性要求较弱的数据. 当经过一段时间之后, 若 GCKS 认为新加入的 sensor 节点是可信的, 则将群组密钥 K 分配给此 sensor 节点. 通过以上过程既可以保证群组消息的安全性, 又可以对新 sensor 节点进行考察. 具体的加入协议描述如下:

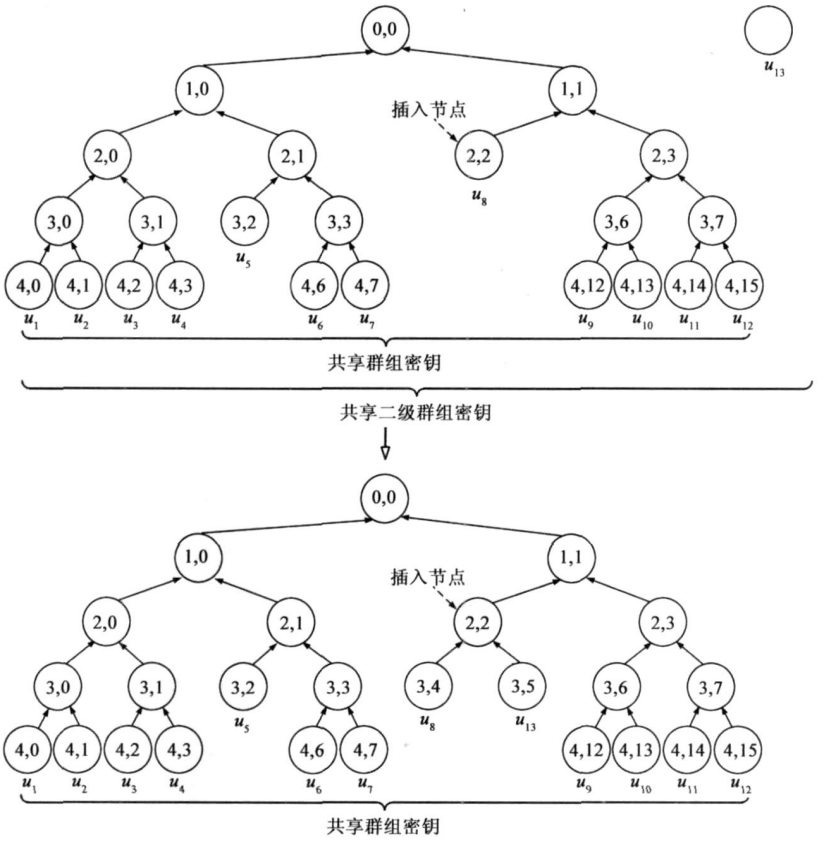


图2　u_{13}加入群组

Join Protocol

Step 1　网络中的 GCKS 根据群组安全策略对 u_{N+1} 进行身份认证.

Step 2　分配二级群组密钥.

Step 2.1　GCKS 生成一个随机数 P, $0<P<p$ 且 P 与 k_{u_1}、k_{u_2}、…、k_{u_N}、$k_{u_{N+1}}$ 两两互素, 并用当前群组密钥 K 加密 P 后把结果发送给网络中的 sensor 节点 $u_1, \cdots, u_{N+1}$.

Step 2.2　令 $k_{u_0}=P$, GCKS 将 $u_1, \cdots, u_N, u_{N+1}$ 的节点密钥 k_{u_1}、k_{u_2}、…、k_{u_N}、$k_{u_{N+1}}$ 和 k_{u_0} 作为中国剩余定理的模数, 并计算相应整数: $M=k_{u_0}k_{u_1}k_{u_2}\cdots k_{u_N}k_{u_{N+1}}$、$M_i=M/k_{u_i}$ 和 M_i 在模 k_{u_i} 下的乘法逆元 M_i', $i=0\sim N+1$. GCKS 随机选择二级群组密钥 K', $0<K'<p$, 利用节点密钥 k_{u_0}、k_{u_1}、k_{u_2}、…、k_{u_N}、$k_{u_{N+1}}$ 计算 $N+2$ 个数 n_0、n_1、n_2、…、n_N、n_{N+1}, 其中 $n_i=k_{u_i}-K'$, $i=0\sim N+1$. 根据 sensor 节点树的节点密钥和群组密钥的选取可知 $0<n_i<k_{u_i}$. GCKS 利用整数 k_{u_i}、n_i、M、M_i 和 M_i' ($i=0\sim N+1$) 计算中国剩余定理的唯一解 $X=(\sum_{i=0}^{N+1}n_iM_iM_i')\bmod M$, 将 X 发送到网络中.

Step 2.3　所有的 sensor 节点计算新的二级群组密钥 $K'=P-(X \bmod P)$.

Step 2.4　u_{N+1} 计算新的二级群组密钥 $K'=k_{u_{N+1}}-(X \bmod k_{u_{N+1}})$.

Step 3　若 u_{N+1} 经过 Δt 时间后没有离开群组且 GCKS 认为 u_{N+1} 是可信的, 则更新群组密钥.

Step 3.1　选择插入节点.

Step 3.1.1　若密钥树是满树, 则生成新的根节点并将其作为插入节点.

Step 3.2.2　否则, 寻找满足如下条件的插入节点: (1) 在插入节点下插入新节点后不会增加树的高度, (2) 尽量使插入节点的位置处于密钥树的

最顶端和最左端.

Step 3.2 GCKS 创建新的中间节点, 将其提升为插入节点和 u_{N+1}的父节点.

Step 4 GCKS 使用 u_{N+1}的节点密钥 $k_{u_{N+1}}$加密其密钥路径上的密钥组并将结果发送给 u_{N+1}.

Step 5 GCKS 使用 u_{N+1}的兄弟节点的节点密钥加密 u_{N+1}的父节点的节点密钥并将结果发送到网络中.

Step 6 所有的 sensor 节点更新密钥树并计算各自密钥路径上的节点密钥.

图 2 给出了成员 u_{13}加入群组的例子, GCKS 进行以下操作:

(1) 生成二级群组密钥, 令原有群组成员和新成员共享此密钥.

经过一段时间之后, 若 GCKS 认为 u_{13}可信, 则进行以下操作:

(2) 将< 2, 2> 重命名为< 3, 4> , 并产生新的群组成员节点< 3, 5> 和中间节点< 2, 2> .

(3) 将< 2, 2> 提升为< 3, 4> 和< 3, 5> 的父节点.

(4) 将< 0, 0> 、< 1, 1> 、< 2, 2> 的节点密钥加密发送给 u_{13}, 将< 2, 2> 的节点密钥加密发送给 u_8.

此后, 所有的节点都可以得到新的节点密钥和群组密钥.

2.3 sensor 节点离开事件

假设具有 N 个 sensor 节点$\{u_1, \cdots, u_N\}$的网络中有 r 个节点离开群组. 离开协议描述如下:

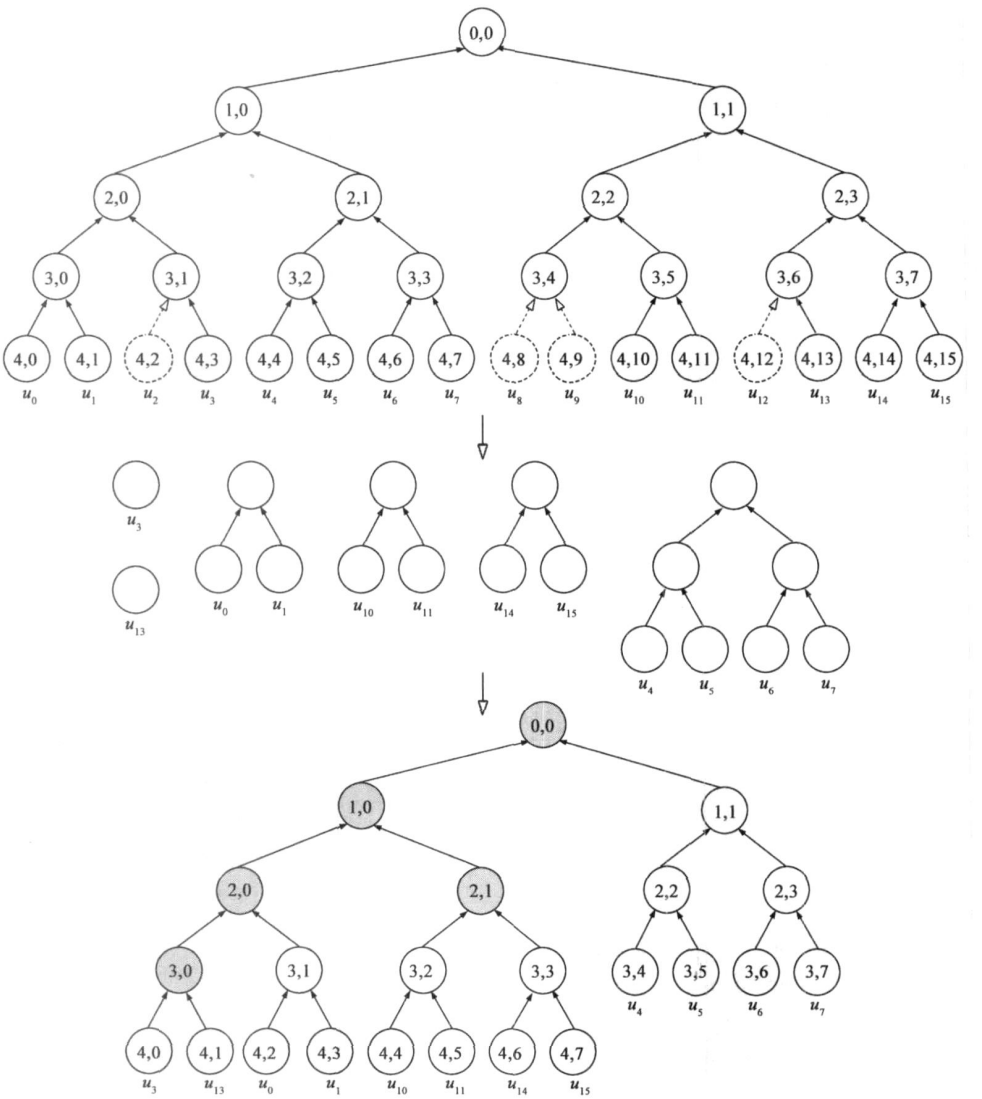


图3 离开事件

Leave Protocol

Step 1　利用完全子集算法[10]把剩余的 sensor 节点对应的密钥树划分成 N' 个互不相交的子树.

Step 2　GCKS 将每个子树的根节点的密钥 k_{r_1}, k_{r_2}, …, $k_{r_{N'}}$ 作为中国剩余定理的模数, 并计算相应整数: $M = k_{r_1} k_{r_2} \cdots k_{r_{N'}}$、$M_i = M / k_{r_i}$ 和 M_i 在模 k_{r_i} 下的乘法逆元 M_i', $i = 1 \sim N'$. GCKS 随机选择新群组密钥 K, $0 < K < p$, 利用节点密钥 k_{r_1}、k_{r_2}、…、$k_{r_{N'}}$ 计算 N' 个数 n_1、n_2、…、$n_{N'}$, 其中 $n_i = k_{r_i} - K$, $i = 1 \sim N'$. 根据 sensor 节点树的节点密钥和群组密钥的选取可知 $0 < n_i < k_{r_i}$. GCKS 利用整数 k_{r_i}、n_i、M、M_i 和 M_i' ($i = 1 \sim N'$) 计算中国剩余定理的唯一解 $X = \left(\sum_{i=1}^{N'} n_i M_i M_i' \right) \bmod M$, 将 X 发送到群组中.

Step 3　更新密钥树.

Step 3.1　确定子树合并顺序.

Step 3.1.1　若密钥树的高度不同, 则先对较矮的树进行合并.

Step 3.1.2　否则, 可以利用某种排列顺序来确定密钥树的合并顺序(如每个密钥树中根节点标识的字典序).

Step 3.2　产生一个新的插入节点, 将最矮的两个密钥树插入到插入节点之下.

Step 3.3　重复 3.2 直到将所有的子树合并为一棵密钥树.

Step 4　GCKS 为每一个新节点 $< l, v >$ 分配节点密钥 $k_{<l, v>}$, 将 $k_{<l, v>}$ 用 $< l, v >$ 的孩子节点 $< l+1, 2v >$、$< l+1, 2v+1 >$ 的节点密钥 $k_{<l+1, 2v>}$、$k_{<l+1, 2v+1>}$ 加密并发送给网络中的 sensor 节点.

Step 5　所有的 sensor 节点得到加密消息后进行解密得到新的节点密钥.

Step 6　所有的 sensor 节点更新密钥树并计算出新的群组密钥 $K = k_{r_i} - (X \bmod k_{r_i})$.

在图 3 的例子中, 假设成员 u_2、u_8、u_9 和 u_{12} 离开群组. 首先通过完全子集算法可以把剩余成员划分为不相交的 5 个集合 $\{u_3\}$、$\{u_{13}\}$、$\{u_0, u_1\}$、$\{u_{10}, u_{11}\}$、$\{u_{14}, u_{15}\}$ 和 $\{u_4, u_5, u_6, u_7\}$. 然后生成新的插入节点 $< 3, 0 >$, 并将最矮的两棵子树插入到 $< 3, 0 >$ 之下, 之后生成新的插入节点 $< 2, 0 >$, 并将刚生成的子树和另外一棵子树插入到 $< 2, 0 >$ 之下, 然后将 $\{u_{10}, u_{11}\}$ 和 $\{u_{14}, u_{15}\}$ 对应的两棵子树插入到新节点 $< 2, 1 >$ 之下. 重复此步骤可以得到最后的密钥树. 之后 GCKS 就可以对群组密钥进行更新.

3　方案分析

3.1　安全性分析

我们提出的群组密钥管理方案的安全性基于如下假设: 当前群组中的每个成员保证其自身私钥 (k_{u_i}) 的安全性, 而 GCKS 保证群组密钥集合的安全性. 而且, 成员私钥是从一个无限大的互素正整数池中随机选择的. 因此, 知道其中的一个私钥并不会得到其他私钥的任何信息.

在第 2 节的方案中, 明文传送的 X 中隐藏了群组密钥或二级群组密钥, 即任何人都可获得 X. 但是在方案中, 攻击者要获得群组密钥, 需要计算 $K = k_{u_i} - (X \bmod k_{u_i})$. 同时由于每个成员的私钥以及密钥树中每个节点的节点密钥都是秘密的, 所以攻击者不能得到这些密钥, 因而攻击者不能计算出群组密钥. 提出的分级群组密钥管理方案的安全性依赖于基于中国剩余定理分发群组密钥的安全性.

本节首先利用信息论工具对群组密钥管理的安全需求进行表述, 然后证明提出的分级群组密钥管理方案满足正确性、群组密钥保密性、前向保密性和后向保密性. 下面的证明过程中 $H(\cdot)$ 表示熵函数.

考虑一个具有 N 个成员 u_1、u_2、…、u_N 和一个 GCKS 的群组. 记每个成员 u_i 掌握的叶子节点密钥 (k_{u_i}) 为个人私钥 $private\_K_i$. 令 m 表示系统所使用的群组密钥数量, R 表示离开成员的集合, 群组密钥 $\{K_{group}^1, K_{group}^2, \cdots, K_{group}^m\}$ 是独立且随机产生的. 对 $j \in \{1, \cdots, m\}$, GCKS 通过多播消息 B_j 将群组密钥 K_{group}^j 发送到群组成员. 对任意的成员 $u_i \in R$, 第 j 个群组密钥 K_{group}^j 由 B_j 和 $private\_K_i$ 确定. 在群组密钥管理方案中, 由于成员 u_i 可能从 B_j 和 $private\_K_i$ 获得比 K_{group}^j 更多的信息, 本节用 $z_{i,j}$ 表示成员 u_i 从 B_j 和 $private\_K_i$ 获得的信息.

定理 1　对于任意成员 u_i, 每个群组密钥 K_{group}^j 都由 $z_{i,j}$ 确定. 更进一步地, K_{group}^j 由 B_j 和 $private\_K_i$ 确定. ($H(K_{group}^j \mid z_{i,j}) = 0$ 且 $H(z_{i,j} \mid B_j, private\_K_i) = 0$) [正确性]

证明: 在提出的群组密钥管理方案中, 任意的成员 u_i 可通过解密多播消息 B_j 得到 $z_{i,j}$, 且 $z_{i,j}$ 包含有关 K_{group}^j 和其他密钥的信息. 所以对任意的群组成员 u_i 都有 $H(K_{group}^j \mid z_{i,j}) = 0$.

在提出的群组密钥管理方案中, 每个加密后的群组密钥 K_{group}^j 和其他信息都通过 B_j 发送给群组成员. 收到加密消息后, 每个群组成员 u_i 都必须使用自己的个

人私钥$private_K_i$解密B_j中的消息得到K^j_{group}和其他信息. 因此对于任意成员u_i, 每个群组密钥K^j_{group}都由B_j和$private_K_i$确定. 但攻击者仅仅通过B_j和$private_K_i$中的一个无法得到$z_{i,j}$中的信息, 即$H(z_{i,j}|B_j, private_K_i)=0$, 但$H(z_{i,j}|B_j)=H(z_{i,j}|private_K_i)=H(z_{i,j})$.

定理 **2** 对于$\{B_1, \ldots, B_m\}$和任意的$K^j_{group}\in\{K^1_{group}, \ldots, K^m_{group}\}$, 攻击者无法确定有关$K^j_{group}$的任何信息. $(H(K^j_{group}|B_1, \ldots, B_m)=H(K^j_{group}))$ [群组密钥保密性]

证明: 假设攻击者从$\{B_1, \ldots, B_m\}$中得到了K^j_{group}. 由于每个K^j_{group}由$z_{i,j}$确定, 即由B_j和$private_K_i$确定. 所以攻击者可以由$\{B_1, \ldots, B_m\}$确定有关B_j和$private_K_i$的相关信息, $j\in\{1, \ldots, m\}$, $i\in\{1, \ldots, N\}$. 但由于任何攻击者都不能确定有关$private_K_i$的任何信息. 即$H(K^j_{group}|B_1, \ldots, B_m)=H(K^j_{group})$.

定理 **3** 已离开群组的成员u_D即使知道原先的群组密钥$\{K^{i_1}_{group}, \ldots, K^{i_v}_{group}\}\subset\{K^1_{group}, \ldots, K^m_{group}\}$, 其也不能够从后续的多播消息$\{B_{i_v+1}, \ldots, B_m\}$中确定有关$\{K^{i_v+1}_{group}, \ldots, K^m_{group}\}$的任何信息. $(H(K^j_{group}|private\_K_D, K^{i_1}_{group}, \ldots, K^{i_v}_{group}, B_{i_v+1}, \ldots, B_m)=H(K^j_{group}), j\in\{i_v+1, \ldots, m\})$ [前向保密性]

证明: 假设成员u_D离开群组, 且其掌握群组密钥$\{K^{i_1}_{group}, \ldots, K^{i_v}_{group}\}$. 当离开协议完成后, GCKS 更新了所有$u_D$掌握的密钥, 即 GCKS 将$u_D$掌握的密钥$\{private_K_D, K^{i_1}_{group}, \ldots, K^{i_v}_{group}\}$从系统中清除. 因此, 此时$u_D$和被动攻击者的攻击能力相同. 从定理 1 和定理 2 可知, $H(K^j_{group}|private_K_D)=H(K^j_{group})$且$H(K^j_{group}|B_{i_v+1}, \ldots, B_m)=H(K^j_{group})$, $j\in\{i_v+1, \ldots, m\}$. 因此, 即使u_D掌握原先的群组密钥$\{K^{i_1}_{group}, \ldots, K^{i_v}_{group}\}$, 其也不能从后续的多播消息$\{B_{i_v+1}, \ldots, B_m\}$中计算当前及以后的群组密钥. 所以提出的方案可以提供前向保密性, 即$H(K^j_{group}|private_K_D, K^{i_1}_{group}, \ldots, K^{i_v}_{group}, B_{i_v+1}, \ldots, B_m)=H(K^j_{group})$, $j\in\{i_v+1, \ldots, m\}$.

定理 **4** 对于一个新群组成员u_i, 即使其掌握当前和后续的群组密钥$\{K^{i_1}_{group}, \ldots, K^{i_v}_{group}\}\subset\{K^1_{group}, \ldots, K^m_{group}\}$, u_i也不能从原先的多播消息$\{B_1, \ldots, B_{i_1-1}\}$中确定有关$\{K^1_{group}, \ldots, K^{i_1-1}_{group}\}$的任何信息. $(H(K^j_{group}|private\_K_i, K^{i_1}_{group}, \ldots, K^{i_v}_{group}, B_1, \ldots, B_{i_1-1})=H(K^j_{group}), j\in\{1, \ldots, i_1-1\})$ [后向保密性]

证明: 在加入事件中, GCKS 产生新的群组密钥$K^{i_1}_{group}$并分别使用原先的群组密钥$K^{i_1-1}_{group}$和u_i的个人私钥$private_K_i$加密新群组密钥. 当u_i收到密钥更新消息后, 利用个人私钥$private_K_i$计算群组密钥$K^{i_1}_{group}$, 进而得到后续的密钥$\{K^{i_2}_{group}, \ldots, K^{i_v}_{group}\}$. 尽管$u_i$可以窃听原先的多播消息$\{B_1, \ldots, B_{i_1-1}\}$, 但其不掌握加密$B_1, \ldots, B_{i_1-1}$的密钥, 所以$u_i$不能解密消息$B_1, \ldots, B_{i_1-1}$. 因此, 对于系统的前期状态来说, 新成员$u_i$和被动攻击者的攻击能力相同. 从定理 1 和定理 2 可知, $H(K^j_{group})=H(K^j_{group}|private_K_i)$且$H(K^j_{group}|K^{i_1}_{group}, \ldots, K^{i_v}_{group})=H(K^j_{group})$, $j\in\{1, \ldots, i_1-1\}$. 因此, u_i不能通过掌握的密钥和原先的多播消息得到原先使用的群组密钥. 所以提出的方案可以提供后向保密性, 即$H(K^j_{group}|private_K_i, K^{i_1}_{group}, \ldots, K^{i_v}_{group}, B_1, \ldots, B_{i_1-1})=H(K^j_{group})$, $j\in\{1, \ldots, i_1-1\}$.

3.2 性能分析

我们的方案希望优化用户的计算量、密钥的存储量和密钥更新的消息数量. 此外, 与其他基于逻辑密钥层次的群组密钥管理相比, 我们的方案比较简单, 只需要使用模运算和乘法运算就可以对密钥进行管理.

由第 2 节的方案, 我们可以得到表 1. 由表 1 可以看到, 提出的方案在运算量、通信量和存储量方面都较小, 适合应用于资源受限的无线传感器网络.

表 **1** 提出方案的性能

提出的方案		加解密运算		模乘运算次数		扩展欧几里德算法	通信轮数	存储密钥的数量	
		GCKS	sensor 节点	GCKS	sensor 节点	GCKS		GCKS	sensor 节点
系统建立		0	0	N	1	N	1	$2N-1$	$\log_2 N$
加入事件	二级群组密钥	1	1	$2+N$	1	$2+N$	1		
	群组密钥	$2\log_2 N$	$\log_2 N$	0	0	0	1		
离开事件		$\log_2 N'$	1	N'	1	N'	1		

4 结束语

本文设计了一种高效的分级群组密钥管理方案来解决 WSNs 中的安全群组通信问题. 首先基于中国剩余定理和密钥树结构给出了一种分级群组密钥管理方案的系统建立过程. 然后介绍了节点加入通信群组时的处理方法: 首先向新成员发送二级群组密钥, 可以让新成员参与一些不太敏感的数据的传送; 若一段时期之后新成员获得 GCKS 的信任, 则向其发送群组密钥, 这时新成员可以真正加入到通信群组. 之后介绍了节点离开时的处理方法, 通过利用完全子集方法将剩余成员进行分割, 提出的方案可以利用中国剩余定理对群组密钥进行安全的更新. 最后对方案的安全性和性能进行了分析, 结果说明此方案适合应用于资源受限的

无线传感器网络.

参考文献:

[1] J H Son, J S Lee, S W Seo. Energy efficient group key management scheme for wireless sensor networks[A]. In Proceedings of the 2nd International Conference on Communication Systems Software and Middleware[C]. Bangalore, India: IEEE Press, 2007. 1-9.

[2] B Panja, S K Madria, B Bhargava. Energy and communication efficient group key management protocol for hierarchical sensor networks[A]. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing[C]. Taichung, Taiwan: IEEE Press, 2006. 384-393.

[3] Z Qingguang, C Yanling, L Juan. A lightweight key management protocol for hierarchical sensor networks[A]. In Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies[C]. Taiwan: IEEE Press, 2006. 379-382.

[4] M Eltoweissy, M H Heydari, L Morales, et al. Combinatorial optimization of group key management[J]. Journal of Network and Systems Management: Special Issue on Network Security, 2004, 12(1): 33-50.

[5] J M Kim, J S Cho, S M Jung, et al. An energy-efficient dynamic key management in wireless sensor networks[A]. In Proceedings of the 9th International Conference on Advanced Communication Technology[C]. Phoenix Park, Korea: IEEE Press, 2006. 2148-2153.

[6] M Moharram, R Mukkamala, M Eltoweissy. TKGS: Threshold-based key generation scheme for wireless Ad Hoc networks[A]. In Proceedings of the IEEE International Conference on Computer Communications and Networking[C]. Chicago, IL, USA: IEEE Press, 2004. 31-36.

[7] R Mukkamala, M Moharram, M Eltoweissy. A novel architecture for secure group communication in wireless Ad-Hoc networks with application-level multicast[A]. In Proceedings of the 3rd International Trusted Internet Workshop[C]. Bangalore, India: 2004.

[8] M F Younis, K Ghumman, M Eltoweissy. Location-aware combinatorial key management scheme for clustered sensor networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2006, 17(8): 865-882.

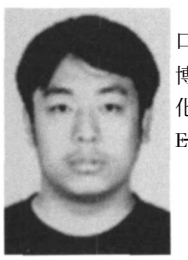
[9] Z Xinliang, H Chirr-Tser, M Manton. Chinese remainder theorem based group key management[A]. In Proceedings of the 45th ACM Southeast Conference(ACMSE 2007)[C]. Winr-storr-Salem, North Carolina, USA: ACM Press, 2007. 266-271.

[10] D Naor, M Naor, J Lotspiech. Revocation and tracing schemes for stateless receivers[A]. In Proceedings of Advances in Cryptology - CRYPTO 2001[C]. Santa Barbara, California, USA: Springer, 2001. 41-62.

作者简介:

李凤华　男, 1966 年 3 月出生于湖北省浠水县, 西安电子科技大学博士生, 北京电子科技学院教授, 主要研究方向为网络安全与可信计算.

E-mail: lfh@besti.edu.cn



王　巍　男, 1980 年 2 月出生于河北省张家口市, 中国电子科技集团公司第三十六研究所, 博士, 主要研究方向为群组密钥管理、协议形式化证明.

E-mail: wwlofty@gmail.com

马建峰　男, 1963 年 10 月出生于陕西省西安市, 西安电子科技大学计算机学院院长、博士、教授、博士生导师, 主要研究方向为密码学与网络安全.

E-mail: jfma@mail.xidian.edu.cn