无线传感器网络中自治愈的群组密钥管理方案

彭清泉[1],裴庆祺[1,2],马建峰[1],庞辽军[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. 中国电子设备系统工程公司研究所,北京 100039)

摘 要: 群组密钥管理的自治愈机制是保证无线传感器网络在不可靠信道上进行安全群组通信的重要手段.基于采用双方向密钥链的群组密钥分发与撤销方法,提出了一个无线传感器网络中具有撤销能力的自治愈群组密钥管理方案.该方案实现了群组密钥的自治愈功能和节点撤销能力,能够满足在较高丢包率的无线通信环境下传感器网络群组密钥管理的安全需求,确保了群组密钥保密性、前向保密性和后向保密性等安全属性.性能分析表明,该方案具有较小的计算和通信开销,能够适用于无线传感器网络.

关键词: 无线传感器网络;安全;群组密钥管理;自治愈
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2010) 01-0123-06

A Self-Healing Group Key Management Scheme in Wireless Sensor Networks

PENG Qing-quan[1], PEI Qing-qi[1,2], MA Jian-feng[1], PANG Liao-jun[1]
(1. *Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi' an, Shaanxi* 710071, *China*;
2. *Institute of China Electronic System Engineering Corporation; Beijing* 100039, *China*)

Abstract: The self-healing mechanism in group key management is an important means that protect secure group communication over lossy channel for wireless sensor networks. Based on group key distribution and revocation method using dual direction key chains, a self-healing group key management scheme with revocation capability for wireless sensor networks is presented. The proposed scheme implements the self-healing function of group key and node revocation capability, and satisfies the desired security requirements of sensor networks group key management in presence of a high losing packet rate of wireless communication environments, such as the group key confidentiality, forward secrecy and backward secrecy. The performance analysis shows that the proposed scheme has less computation cost and communication cost, suitable for wireless sensor networks.

Key words: wireless sensor networks; security; grqoup key management; self-healing

1 引言

无线传感器网络由大量造价低、能量有限、计算和通信能力弱的传感器节点组成,这些资源受限的节点通常需要以分组的方式进行有效协作,由此决定了群组通信是它的主要通信方式之一.而无线传感器网络一般部署在无人照看甚至敌对的环境下,攻击者容易利用无线通信的脆弱性对网络通信实施攻击,因此,保证群组通信的安全性是无线传感器网络安全服务中重要的研究内容.

为保证无线传感器网络中群组通信的安全性,需要在传感器群组内所有成员节点之间共享一个群组会话密钥.传感器网络中群组密钥管理的目的就是让群组中的所有成员安全的共享一个群组会话密钥,同时对成员的加入与撤销进行处理,确保群组密钥的前向保密性和后向保密性.目前,针对传统有线网络和无线网络中群组密钥管理的研究已经取得了许多成果,提出了多种安全高效的群组密钥管理协议和算法[1~3].但是,这些技术并不能很好的直接应用于无线传感器网络环境.无线传感器网络中的群组通信一般是在不可靠的敌对环境中进行,传感器节点易受到各种攻击,而且传输过程中数据包容易被丢失.因此,无线传感器网络群组通信应该考虑如何处理传输过程中数据包丢失的问题.在无线传感器网络安全群组通信方面一个重要的研究成果是 Perrig 等人提出的 μTESLA 协议[4],该协议采用延迟密钥公布机制,仅用对称密码体制就实现了高效的广播认证,但是它存在密钥延迟暴露和非实时认证的问题,容易受到 DoS 攻击.Park 等人提出了一个适用于传感器网络的轻量级安全协议模型(LiSP)[5],该模型给出了一种

收稿日期:2008-12-02;修回日期:2009-02-27
基金项目:国家自然科学基金重大计划(No.60633020);国家自然科学基金(No.60803151);NSFC-广东联合基金重点项目(No.U0835004);高等学校学科创新引智计划(No.B08038)

具有广播认证和自动恢复密钥更新消息的算法,但是它没有考虑密钥恢复过程中节点撤销的安全性问题. Jiang 等人[6]最近提出了一个无线传感器网络中节点可在有限时间内被撤销的群组密钥分发方案,该方案实现了具有隐式认证的群组密钥周期性更新,但它需要在每个节点加入群组通信之前预先确定其生命周期,而且在有效生命周期内的叛逆节点不能及时被撤销.

Staddon 等人[7]在 2002 年最早提出来自治愈的群组密钥分发思想:在群组密钥分发过程中,群组密钥分发广播消息仅仅对被授权的群组成员是有用的,合法群组成员结合预先分配的个人秘密信息能够从广播消息中恢复出共享的群组会话密钥,而被撤销的和未被授权的非法用户从广播消息中则不能得到有关群组会话密钥的信息,合法群组成员在离线一段时间后再重新返回群组时,不需要重传额外的信息就能够立即恢复出丢失的群组会话密钥.自治愈机制在无线传感器网络群组密钥管理中具有重要的研究价值.文献[7]最先提出可撤销的自治愈群组密钥分发的形式化定义、资源占用下界以及几个构造方案;之后,许多改进的自治愈群组密钥分发技术与方案被提出来[8~10].其中,Liu 等人[8]推广了自治愈群组密钥分发的定义,通过引入一个新的个人秘密信息分发技术,提出了一个具有可撤销能力的高效的自治愈群组密钥分发方案,减少了通信负载和存储开销;文献[9]基于单向密钥链,提出了一个新的自治愈群组密钥分发方法,并设计了一个具有较少计算和通信开销的计算上安全的自治愈群组密钥分发方案;文献[10]提出了一种基于向量空间访问结构上的秘密共享方法.

本文在采用双向密钥链的自治愈群组密钥分发方法的基础上,提出了一个无线传感器网络中具有撤销能力的自治愈群组密钥管理方案.该方案通过双向密钥链和广播多项式实现了群组密钥管理的自治愈属性和对叛逆节点的可撤销能力,能够满足无线传感器网络中在具有较高丢包率的无线通信环境下的群组密钥管理的安全需求,并确保群组密钥保密性、前向保密性和后向保密性等安全属性.同时,该方案实现了群组密钥无缝更新过程,在密钥更新过程中不会中断数据的传输.性能分析表明,该方案具有较小的计算和通信开销,能够适用于无线传感器网络安全群组通信.

2 群组密钥的分发与撤销

2.1 单向密钥链与双方向密钥链

单向密钥链是反复用一个单向散列函数 H 作用到一个随机密钥种子上而产生的密码学安全的密钥链[11].单向散列函数 H 能够把任意长的二元字符串变换成固定长的二元字符串,它满足以下两条基本性质:(1)给定 x,计算出 $y = H(x)$ 是容易的;(2)给定 y,要计算出满足 $H(x) = y$ 的 x 在计算上是不可行的.构造一条长度为 m 的单向密钥链 $\{K_1, K_2, \cdots, K_m\}$,GKS 首先随机选取一个密钥种子 K_0,然后计算出 $K_1 = H(K_0), K_2 = H(K_1), \cdots, K_m = H(K_{m-1})$.由于散列函数 H 的单向性,已知 K_i,对于任意 $j < i$,得出 K_j 在计算上是不可行的,但对于任意 $j > i$,能有效计算出 $K_j = H^{j-i}(K_i)$.

双方向密钥链是由两条长度相同的单向密钥链组成,其中一条为前向密钥链(forward key chain, K^F),另一条为后向密钥链(backward key chain, K^B).如图 1 所示,给定两个随机密钥种子 K_0^F 和 K_0^B,可以生成一个双方向密钥链 $\{K_1^F, K_2^F, \cdots, K_m^F\}$ 和 $\{K_1^B, K_2^B, \cdots, K_m^B\}$,其中前向密钥链 $K_i^F = H(K_{i-1}^F) = H^{i-1}(K_0^F)$,后向密钥链 $K_i^B = H(K_{i-1}^B) = H^{i-1}(K_0^B)$.

2.2 群组密钥的分发与撤销方案

基于文献[8,9]的工作,给出一个采用双方向密钥链的具有自治愈属性的群组密钥分发与撤销方案.假设无线传感器网络中每个节点都有一个唯一的身份标识号 i,每个通信群组由 n 个节点集合 $U = \{U_1, U_2, \cdots, U_n\}$ 组成,其中 U_i 是身份标识号为 i 的群组成员;F_q 为一个有限域,q 为一个大的素数;H 为密码学上安全的单向散列函数.

(1)初始化设置　群组密钥服务器 GKS 首先从 F_q 中随机选取一个前向密钥种子 K_0^F 和一个后向密钥种子 K_0^B.然后利用单向散列函数 H 分别反复作用在 K_0^F 和 K_0^B 上,计算出两条长度都为 m 的单向密钥链:$K_i^F = H(K_{i-1}^F) = H^{i-1}(K_0^F)(1 \leqslant i \leqslant m)$ 和 $K_i^B = H(K_{i-1}^B) = H^{i-1}(K_0^B)(1 \leqslant i \leqslant m)$.在第 j 次会话中的群组密钥可以通过公式:$GK_j = K_j^F + K_{m-j+1}^B$ 计算得到.GKS 然后均匀、独立地选取 m 个 t 次多项式 $s_1(x), \cdots, s_m(x) \in F_q(x)$,其中 t 为系统参数并且 $t < m, n$.GKS 再通过安全信道向每一个群组成员 U_i 发送节点秘密信息 $S_i = \{s_1(i), \cdots, s_m(i), K_0^F\}$.

(2)密钥分发广播　令 $R_j = \{U_{r_1}, \cdots, U_{r_{w_j}}\}$ 表示在第 j 次会话及其之前所有会话中被撤销用户的集合,并且满足条件 $|R_j| = w_j \leqslant t$.在第 j 次会话中,GKS 从后向密钥链中得到后向密钥 K_{m-j+1}^B,并且计算出撤销多项式:$r_j(x) = (x - r_1)\cdots(x - r_{w_j})$ 和广播多项式 $g_j(x) = r_j(x)$

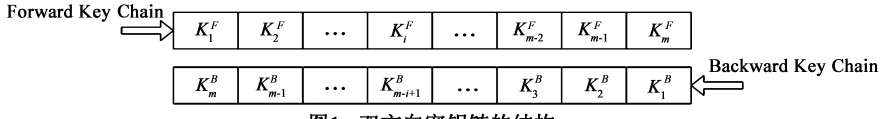

图1　双方向密钥链的结构

$\cdot K^B_{m-j+1} + s_j(x)$. GKS 然后向群组内发送广播消息 $B_j = \{R_j\} \cup \{g_j(x)\}$.

(3)群组会话密钥恢复　当群组中一个未被撤销的用户 U_v 在收到群组密钥分发广播消息 B_j 时,它首先计算撤销多项式 $r_j(x)$在点 v 的值 $r_j(v)$及广播多项式的值 $g_j(v)$,然后结合节点秘密信息 $s_j(v)$,并通过计算公式:

$$K^B_{m-j+1} = \frac{g_j(v) - s_j(v)}{r_j(v)}$$

恢复出后向密钥 K^B_{m-j+1}. U_v 再利用节点秘密信息中的前向密钥种子 K^F_0 计算出前向密钥 $K^F_j = H^{j-1}(K^F_0)$. 最后可以恢复出当前群组会话密钥 $GK_j = K^F_j + K^B_{m-j+1}$.

(4)新的群组成员加入　当 GKS 需要在第 j 次会话中增加新的群组成员时,只要随机选取一个未被使用过的节点身份标识号 $v \in F_q$,并计算 $s_j(v), s_{j+1}(v), \cdots, s_m(v)$,然后将节点秘密信息$\{v, s_j(v), \cdots, s_m(v), K^F_j\}$通过安全信道发送给新加入的节点,就完成了新的群组成员加入操作.

(5)重新初始化设置　当 m 次会话周期执行完之后或者群组中被撤销的用户超过系统参数 t 之后,群组通信需要按照(1)中的步骤重新进行初始化设置.

(6)自治愈机制　令 $1 \leqslant j_1 < j \leqslant j_2$,当群组成员 U_i 分别收到会话 j_1 和 j_2 的群组密钥分发广播消息 B_{j_1}和 B_{j_2},但没有收到会话 j 中的广播消息 B_j 时,U_i 仍然能够通过以下步骤恢复出所有丢失的群组会话密钥 $K_j(j_1 < j < j_2)$: U_i 首先从会话 j_2 收到的广播消息 B_{j_2}中恢复出 $K^B_{m-j_2+1}$,对 $K^B_{m-j_2+1}$应用单向散列函数 H 计算出后向密钥链 $K^B_{m-j+1}(j_1 \leqslant j < j_2)$;然后,通过对前向密钥种子 K^F_0 反复应用单向杂凑函数 H 可以计算出前向密钥链 K^F_j $(j_1 \leqslant j \leqslant j_2)$;最后,$U_i$ 可以恢复出所有丢失的群组会话密钥 $GK_j = K^F_j + K^B_{m-j+1}(j_1 \leqslant j \leqslant j_2)$.

(7)节点撤销机制　当某个节点 U_i 在会话 j_1 中被 GKS 撤销后,对于这之后的任意会话 $j > j_1$, U_i 只能计算出前向密钥 K^F_j,而由于 $r_j(i) = 0$,它不能计算出后向密钥 K^B_{m-j+1},从而使得 U_i 不能得到随后的群组会话密钥 $GK_j(j > j_1)$,因此该群组密钥分发方案隐含了节点撤销功能.

3　无线传感器网络中自治愈的群组密钥管理方案

3.1　无线传感器网络群组通信模型

无线传感器网络中通常有两种类型的节点,一类是能量敏感、计算和通信能力弱的资源有限的传感器节点,另一类则是具有较强计算能力、较多能量的资源相对丰富的基站节点. 一般情况下,传感器节点被部署在监测区域采集数据,而基站节点则用于收集传感器节点的监测数据并将其传送到外部网络. 在无线传感器网络中传感器节点通过静态或者动态的方式形成一个个通信群组,资源相对丰富的基站则作为群组管理员(GM)负责群组拓扑管理,同时作为群组密钥管理服务器(GKS)负责控制群组通信的安全. 在每个群组内 GKS 和所有的群组成员节点之间共享一个群组密钥(GK),用于控制对群组内多播通信数据的访问. 同时,在群组内 GKS 和每一个群组成员节点之间预先分配一个对称秘密密钥(SK). 每一个通信群组的生命周期被划分成 m 次会话,每次会话的时间间隔为 T. 群组密钥在每一次会话中被周期性的更新.

无线传感器网络群组通信基本安全需求包括:(1)群组密钥的保密性:确保群组外部的传感器节点不能访问该群组的群组密钥;(2)前向保密性:确保被撤销的传感器节点不能得到其离开后的群组会话密钥;(3)后向保密性:确保新加入群组的传感器节点不能得到其加入之前的群组会话密钥.

3.2　自治愈的群组密钥管理方案

针对无线传感器网络群组通信模型和安全需求,提出一个具有自治愈属性和节点撤销能力的群组密钥管理方案. 如图 2 所示,方案由群组密钥分发与撤销、密钥认证与恢复、密钥交换三个模块组成.

在群组密钥分发与撤销模块采用第 3 节中描述的可撤销的群组密钥分发方案,该方案能够通过一次广播消息,同时满足群组密钥的分发和节点的撤销. 密钥认证与恢复模块的核心思想是在每个传感器节点中预先分配能够容纳 $l+2$ 个群组密钥的内存缓冲区,群组密钥服务器 GKS 只需广播一条消息,成员节点就能够从双方向密钥链中恢复出群组会话密钥,从而能够容忍不可靠广播信道中的包的丢失;当群组密钥分发广播包丢失或者认证失效时,节点不需要群组密钥服务器 GKS 重传数据包就可以自动恢复出丢失的群组密钥. 密钥交换模块通过为每个节点分配两个可以并发操作的密钥槽,从而能够无缝的交换群组会话密钥而

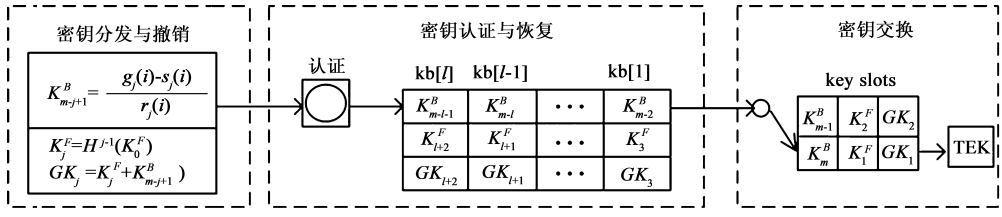

图2　自治愈群组密钥管理方案

不中断数据传输的连续性,在密钥更新中交替分配其中一个密钥槽用于存储当前的群组会话密钥.方案具体可以分为以下几部分:

3.2.1 初始化配置

在群组密钥建立初始化阶段,在群组密钥服务器 GKS 和每个节点 U_i 之间通过实体认证预先共享了一个对称秘密密钥 SK_i,用于初始化消息加密和认证.群组密钥服务器 GKS 首先从 F_q 中随机选取两个密钥种子 K_0^F 和 K_0^B,并利用单向散列函数 H 计算出后向密钥链 $K_i^B = H(K_{i-1}^B) = H^{i-1}(K_0^B)(1 \leqslant i \leqslant m)$.GKS 然后均匀、独立地选取 m 个 t 次多项式 $s_1(x),\cdots,s_m(x) \in F_q(x)$,$t$ 为系统参数并且 $t < m, n$.系统初始设置时,GKS 发送下面消息给每一个群组成员 U_i:

$$\mathrm{GKS} \rightarrow U_i: E_{SK_i}(l \mid K_{m-l-1}^B \mid K_0^F \mid s_m(i) \mid \cdots \mid s_{l+3}(i) \mid T)$$
$$\mid MAC(l \mid K_{m-l-1}^B \mid K_0^F \mid s_m(i) \mid \cdots \mid s_{l+3}(i) \mid T)$$

其中 l 是节点密钥缓冲区的长度,T 为密钥更新的周期.当节点 U_i 收到初始化消息后,执行如下操作:

(1)利用与 GKS 共享的对称秘密密钥 SK_i 解密收到的初始化消息,得到参数:l,T,K_{l+2}^B,K_0^F,$s_m(i),\cdots,s_{l+3}(i)$;(2)分配长度为 l 的缓冲区(kb[1],…,kb[l])和两个密钥槽(ks[1],ks[2]);(3)应用单向散列函数 H 作用于 K_{m-l-1}^B 计算出密钥链:$\{K_{m-l-1}^B, K_{m-l}^B, \cdots, K_m^B\}$,并将这些密钥存储在密钥缓冲区中;(4)计算 $GK_1 = H(K_0^F) + K_m^B$ 作为当前活动的加密密钥;(5)设置密钥更新定时器为 $T/2$;(6)当定时器过期时,计算 $GK_2 = H^2(K_0^F) + K_{m-1}^B$ 作为当前活动密钥,右移动密钥缓冲区自动更新数据加密密钥.

3.2.2 群组密钥周期性更新与恢复

群组密钥建立初始设置之后,GKS 周期性的向群组内的节点广播群组密钥更新消息,在群组会话 $j(j \geqslant 1)$中,GKS 向群组内所有节点广播密钥更新消息:

$$\mathrm{GKS} \rightarrow *: \{R_j\} \bigcup \{g_j(x) = r_j(x) \cdot K_{m-j-l-1}^B + s_{j+l+2}(x)\}$$

其中,R_j 表示会话 j 及其之前会话中所有被撤销节点的集合,$r_j(x) = (x - r_1)\cdots(x - r_{w_j})$ 为撤销多项式.当节点 U_i 收到密钥更新广播消息后,执行如下操作:

(1)通过接收到的 $g_j(x)$ 和身份标识 i 计算出 $g_j(i)$,再利用初始设置时收到的节点秘密信息 $s_{j+l+2}(i)$,根据计算公式:

$$K_{m-j-l-1}^B = \frac{g_j(i) - s_{j+l+2}(i)}{r_j(i)}$$

从而恢复出后向密钥 $K_{m-j-l-1}^B$;(2)对恢复出的 $K_{m-j-l-1}^B$ 进行单向散列函数运算,如果对于任意 $e(0 \leqslant e < l)$,都不存在一个 w 使得等式 $H^{e+1}(K_{m-j-l-1}^B) = K_w^B$ 成立,则广播消息认证失效,丢弃本次接收到的广播消息;如果存在一个 w 使得等式成立,则该次广播消息将作为会话 $j + l + 2$ 的密钥更新消息使用,并被放到密钥缓冲区中;(3)将 kb[1]中密钥移动到非活动的密钥槽,然后将所有的密钥缓冲区中的密钥做右移操作;(4)如果满足(2)中等式的 $e \neq 0$,即存在 e 个丢失的密钥分发广播消息,则通过计算 $H^i(K_{m-j-l-1}^B) \rightarrow \mathrm{kb}[l - i](0 \leqslant i \leqslant e)$恢复出丢失的密钥信息;(5)通过 $GK_j = H^j(K_0^F) + K_{m-j}^B$ 作为当前活动密钥进行加密.

3.2.3 群组成员动态加入与撤销

当一个新的节点 U_v 要在第 j 次会话中加入一个群组时,需执行如下操作:

(1)GKS 首先对 U_v 进行实体认证,认证通过后在节点 U_v 和 GKS 之间建立了一个共享对密钥 SK_v.

(2)GKS 通过群组密钥初始化消息将当前系统配置信息发送给 U_v:

$$GKS \rightarrow U_v: E_{SKv}(l \mid K_{m-j-l-1}^B \mid K_j^F \mid s_{m-j+1}(v) \mid \cdots \mid s_{l+j+2}(v) \mid T)$$
$$\mid MAC(l \mid K_{m-j-l-1}^B \mid K_j^F \mid s_{m-j+1}(v) \mid \cdots \mid s_{l+j+2}(v) \mid T)$$

(3)当 U_v 收到 GKS 发来的初始化消息后,它就可执行群组密钥设置和周期性更新操作加入群组通信.

当 GKS 在会话 j 中检测到节点 U_r 被攻击需要将其撤销时,U_r 的身份 ID_r 会出现在密钥更新广播消息的撤销集合 R_j 中,由于它不能从密钥更新广播消息中恢复出后续的群组密钥,从而隐式的从群组中被撤销.

3.2.4 重新初始化配置

当双方向密钥链中的 m 个群组密钥使用完之后,或者群组中叛逆的节点超过了系统参数 t,那么该群组中的所有节点需要按照 3.2.1 节中的步骤重新进行初始化配置.如果其中某个节点因丢失的密钥广播消息超过了缓冲区长度 l 而发送请求密钥更新消息时,则只需要 GKS 向该节点单播当前会话密钥信息.

4 安全性分析

提出的方案能够满足传感器网络群组密钥管理的安全需求,包括群组密钥的保密性、前向保密性、后向保密性等.

(1)群组密钥的保密性 在第 j 次会话密钥周期性更新过程中,节点的群组会话密钥为 $GK_j = K_j^F + K_{m-j+1}^B$,其中 $K_j^F = H^{j-1}(K_0^F)$,$K_j^B = H^{j-1}(K_0^B)$,K_0^F 是系统初始化设置时 GKS 发给群组成员节点的前向密钥种子,K_0^B 是秘密的后向密钥种子.由于后向密钥 K_{m-j+1}^B 在群组密钥分发广播消息中被节点秘密信息隐藏起来,被动攻击者由于不能有效得到群组成员节点的私有秘密信息,从而不能恢复出群组密钥,因此保证了只有经过认证的群组成员节点能够有效得到群组会话密钥;**(2)前向保密性** 由于密钥链的单向性,当 $j_2 > j_1$

时,从 $K_{j_2}^B$中计算出 $K_{j_1}^B$在计算上是不可行的.因此,被撤销的传感器节点在离开群组后即使知道后向密钥 K_m^B,…,K_{m-j+2}^B,也不能计算出 K_{m-j+1}^B,从而不能恢复出其被撤消后的群组会话密钥;**(3)后向保密性** 在第 j 次周期会话中新加入的群组成员节点,只能得到前向密钥链中的 K_j^F,而对于任意的 $j_1 < j$,由于 $K_j^F = H^{j-j_1}(K_{j_1}^F)$ 以及密钥链的单向性,从 K_j^F 计算出 $K_{j_1}^F$在计算上是不可行的.因此,在群组会话 j 中新加入的节点即使知道前向密钥 K_j^F,…,K_m^F,也不能计算出 $K_{j_1}^F(j_1 < j)$,从而不能恢复出其加入之前的群组会话密钥.

5 方案性能分析

5.1 节点状态稳态分布模型

为了分析方案中传感器节点的计算开销以及密钥服务器与节点之间的通信开销,首先引入马尔可夫(Markov)链的稳态分布模型[5].在无线传感器网络中由于信道的不稳定可能导致群组密钥分发消息数据包丢失或者节点接收到密钥分发消息而认证失效的情况,假设这两种情况具有相同的概率,可以当成是一个独立随机事件.因此,每个传感器节点的密钥缓冲区状态可以简单模型化为一维马尔可夫链,如图3所示.其中,状态 $i(0 \leqslant i \leqslant t)$表示在节点的密钥缓冲区中存在 i 个空槽.当密钥分发消息数据包丢失或者成功接收到密钥更新消息事件发生时,节点状态发生转移.用 p_s 表示成功接收到密钥更新消息的概率,p_l 表示某一次密钥分发消息丢失或者认证失效的概率,且 $p_s = 1 - p_l$.

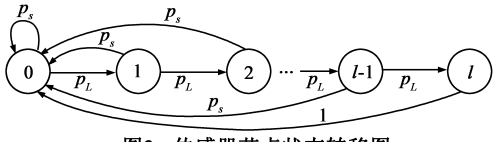

图3 传感器节点状态转移图

令 $p(i)$表示节点在状态 i 的稳态概率,$p_e(k)$表示节点密钥缓冲区中有 k 个空槽的概率,则有:

$$p_e(k) = \sum_{k=0}^{l} p(i) \tag{1}$$

$$\sum_{k=0}^{l} p_e(k) = 1 \tag{2}$$

根据全局平衡方程可以得到:

$$p(i) = p(i-1) \cdot p_L, i = 1, \cdots, l \tag{3}$$

$$p(0) \cdot p_L = p(l) + \sum_{k=0}^{l-1} p(i) \cdot p_S \tag{4}$$

由式(1)(3)(4)可以推导出:

$$p_e(k) = (p_L)^k \cdot p(0), k = 0, \cdots, l \tag{5}$$

由式(2)(5)可以得出:

$$p(0) = (1 - p_L)/(1 - (p_L)^{l+1}) \tag{6}$$

5.2 节点计算开销

由于传感器网络中群组成员节点具有相对较少的计算资源,因此只考虑传感器成员节点上的计算开销.方案中每个成员节点的计算开销主要包括多项式求值、求和操作以及 Hash 运算,但是前两项的计算开销相对较小且是固定的,在此主要通过每次密钥更新过程中的 Hash 运算量来分析节点的计算开销.

令 N^H 表示每次密钥更新过程中节点所需执行的 Hash 运算次数.当节点中有 k 个空槽时,N^H 的条件期望值为:

$$E[N^H \mid k \text{ empty slots}] = \begin{cases} (k+1) \cdot p_S + 0 \cdot p_L = (k+1) \cdot (1 - p_L), k < l \\ (l+1) \cdot p_S + (l+1) \cdot p_L = l + 1, k = l \end{cases} \tag{7}$$

根据期望值计算公式有:

$$E[N^H] = \sum_{k=0}^{l} E[N^H \mid k \text{ empty slots}] \cdot p_e(k) \tag{8}$$

由式(5)(6)(7)和(8)可以得出节点每次密钥更新所需执行 Hash 运算的期望值为:

$$E[N^H] = (l+1) \cdot (p_L)^l \cdot (1 - p_L)/(1 - (p_L)^{l+1}) + \sum_{k=0}^{l-1} (k+1) \cdot (p_L)^k \cdot (1 - p_L)^2/(1 - (p_L)^{l+1}) \tag{9}$$

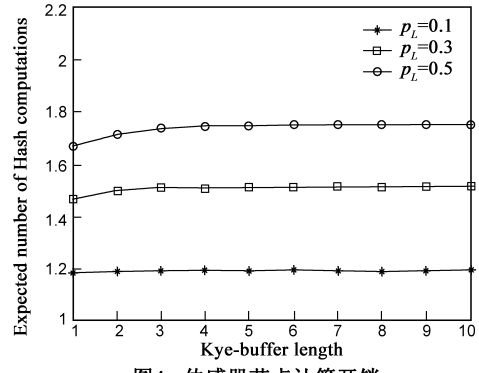

图4 传感器节点计算开销

图4给出了当 p_L 取不同值时,$E[N^H]$作为密钥缓冲区长度 l 的函数图形.从图中可以看出,即使在信道丢包率很大的情况下(如 $p_L = 0.5$),每次密钥更新节点平均也只需较小的计算开销.

5.3 通信开销

群组密钥服务器 GKS 和成员节点之间的通信开销主要包括系统初始化配置时秘密分发消息所需通信开销 C_{init}和群组密钥更新过程中广播消息所需通信开销 C_{update}.当 m 个周期会话密钥全部使用完或者 l 个密钥缓冲区全为空时,GKS 需要重新进行初始化设置通信,而其它的情况下则只需周期性的广播群组密钥分发消息,由此可以得出每个节点与 GKS 之间的通信开销期望值 $E(C)$为:

$$E(C) = C_{init} \cdot (1/m + p_e(l)) + C_{update} \cdot \sum_{k=0}^{l-1} p_e(k) \tag{10}$$

令 $\alpha = C_{init}/C_{update}$,用 C_{update}对式(10)进行归一化处理可以得到:

$$C = \alpha \cdot (1/m + p_e(l)) + \sum_{k=0}^{l-1} p_e(k) \qquad (11)$$

由式(5)(6)(11)可以得到:

$$C = \alpha \cdot (1/m + (p_L)^l \cdot (1 - p_L)/(1 - (p_L)^{l+1})) + \sum_{k=0}^{l-1} (p_L)^k \cdot (1 - p_L)/(1 - (p_L)^{l+1}) \qquad (12)$$

图 5 给出了当 p_L 取不同值时,归一化通信开销 C 作为密钥缓冲区长度 l 的函数的图形,其中 $\alpha = 10$, $m = 100$. 从图中可以看出,节点的密钥缓冲区长度 l 越大所需的通信开销越小.

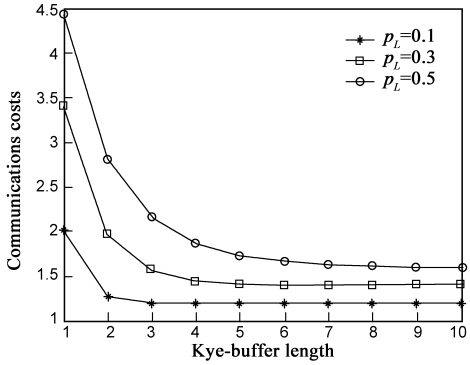

图5 群组节点的通信开销

6 结论

随着无线传感器网络的应用不断深入和广泛,缺少有效的安全机制已成为制约其发展的主要障碍之一. 群组密钥管理作为传感器网络中一项重要的安全服务而备受研究关注. 本文提出了一个传感器网络中具有撤销能力的自治愈群组密钥管理方案,该方案采用了基于双方向密钥链的自治愈的群组密钥分发与撤销方法,通过双方向密钥链和广播多项式实现了群组密钥的自治愈属性和节点撤销能力,能够满足无线传感器网络中在具有较高丢包率的无线通信环境下的群组密钥管理的安全属性. 同时,该方案具有较小的计算和通信开销,能够适用于资源受限的无线传感器网络应用环境.

参考文献:

[1] Rafaeli S, Hutchison D. A survey of key management for secure group communication[J]. ACM Computing Surveys, 2003, 35(3): 309 – 329.

[2] Challal Y, Seba H. Group key management protocols: a novel taxonomy[J]. International Journal of Information Technology, 2005, 2(1): 105 – 119.

[3] Wang W, Li F, Ma J. Efficient and secure group key management for high delay networks[J]. Chinese Journal of Electronics, 2007, 16(4): 721 – 726.

[4] Perrig A, Szewczyk R, Wen V, et al. SPINS: security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521 – 524.

[5] Park T, Shin K G. LiSP: a lightweight security protocol for wireless sensor networks[J]. ACM Transactions on Embedded Computing Systems, 2003, 3(3): 634 – 660.

[6] Jiang Y, Lin C, Shen X, et al. Self-healing group key distribution with time-limited node revocation for wireless sensor networks[J]. Ad Hoc Networks (Elsevier), 2007, 5(1): 14 – 23.

[7] Staddon J, Miner S, Franklin M, et al. Self-healing key distribution with revocation[A]. Proceedings of IEEE Symposium on Security and Privacy'02[C]. Los Alamitos: IEEE Press, 2002. 224 – 240.

[8] Liu D, Ning P, Sun K. Efficient self-healing group key distribution with revocation capability[A]. Proceedings of the 10th ACM Conference on Computer and Communications Security[C]. New York: ACM, 2003. 231 – 240.

[9] Dutta R, Chang E. C, Mukhopadhyay S. Efficient self-healing key distribution with revocation for wireless sensor networks using one way key chains[A]. Proceedings of the 5th International Conference on Applied Cryptography and Network Security[C]. LNCS 4521, Berlin: Springer-Verlag, 2007. 385 – 400.

[10] Dutta R, Mukhopadhyay S, Das A, et al. Generalized self-healing key distribution using vector space access structure[A]. NETWORKING 2008[C]. LNCS 4982, Berlin: Springer-Verlag, 2008. 612 – 623.

[11] Lamport L. Password authentication with insecure communication[J]. Communications of the ACM, 1981, 24(11): 770 – 772.

作者简介:

彭清泉 男,1980 年出生于江西高安,博士研究生. 主要研究方向为无线网络安全、安全协议.
E-mail: qingquanpeng@sina.com

裴庆祺 男,1975 年出生于广西陆川,博士,副教授. 主要研究方向为信息安全、传感器网络及安全.
E-mail: qqpei@mail.xidian.edu.cn

马建峰 男,1963 年出生于陕西西安,博士,教授、博士生导师. 主要研究方向为计算机安全、密码学、移动与无线网络安全.

庞辽军 男,1978 年出生于陕西渭南,博士,副教授. 主要研究方向为密码学、电子商务中的安全理论与技术.
E-mail: ljpang@mail.xidian.edu.cn