基于增强型双向散列链的自愈组密钥分发方案*

覃荣华[1,2], 何亮明[1,2], 杨 旭[1], 袁晓兵[1]

(1. 中国科学院上海微系统与信息技术研究所 无线传感网实验室, 上海 200050; 2. 中国科学院大学 计算与通信工程学院, 北京 100049)

摘 要: 针对基于传统双向散列链的自愈组密钥分发方法无法抵制合谋攻击的不足,提出了引入滑动窗口和轻量级子链 LiBHC 结构的增强型双向散列链结构,并给出了基于该结构的自愈组密钥分发方案。该方案有效地解决了组密钥的无缝切换问题,更大程度地减少了合谋攻击对系统构成的安全威胁。分析表明,本方案在保持较好的资源开销优势的前提下,获得了更好的安全性和可靠性,更适用于节点俘获攻击多发的应用场景。

关键词: 无线传感器网络; 组密钥分发; 增强型双向散列链; 合谋攻击; 节点撤销; 自愈

中图分类号: TP393.08 **文献标志码:** A **文章编号:** 1001-3695(2012)09-3460-04

doi:10.3969/j.issn.1001-3695.2012.09.069

Self-healing group key distribution scheme based on enhanced dual directional hash chains

QIN Rong-hua[1,2], HE Liang-ming[1,2], YANG Xu[1], YUAN Xiao-bing[1]

(1. *Wireless Sensor Network Laboratory, Shanghai Institute of Micro-system & Information Technology, Chinese Academic of Science, Shanghai* 200050, *China*; 2. *College of Computation & Communication Engineering, University of Chinese Academic of Sciences, Beijing* 100049, *China*)

Abstract: The conventional dual directional hash chains based self-healing group key distribution schemes are vulnerable to the collusion attack. To overcome the problem, this paper introduced EDDHC, which consisted of a slide window and a light weight sub-chain (LiBHC). The paper also used EDDHC to design the group key distribution scheme. The proposed scheme enabled the seamless switching of the group key in used and the greater reduction of security vulnerability to the collusion attack. The analysis illustrates that the scheme maintains low resource overhead while achieving better reliability and security performance.

Key words: wireless sensor networks(WSN); group key distribution; enhanced dual directional hash chains(EDDHC); collusion attack; node revocation; self-healing

无线传感器网络(WSN)由大量的集成化微型传感器节点组成,能够协作地实时监测、感知和采集各种环境或者监测对象信息。WSN 在各个领域的广泛应用,引起了人们对大规模动态拓扑网络的密钥分发机制的关注与研究。WSN 分组结构网络进行安全多播信息交换需要使用组密钥对信息报文进行加密。按会话进行组密钥更新,将会给系统带来更理想的安全性。因此,具有自愈能力的组密钥分配方案在密钥管理领域也成为一个研究热点。

1 相关研究进展

自 2002 年 Staddon 等人[1]提出自愈密钥分发方案以来,Liu、Blundo、Dutta、Tian 等人[2~5]提出了一系列的非状态依赖型自愈组密钥分配方案和改进方案。自愈组密钥分发方案根据其理论基础可以分为五种类别[6],即多项式秘密共享、向量空间秘密共享、散列链、SDR(subset difference rekeying)和双线性对。基于向量空间秘密共享[7]和基于双线性对[8],正如文献[6]的分析,这些类别的组密钥分发方案可以达到很好的安全等级,但却会造成较大的通信开销或计算开销。而基于散列链的组密钥分发方法在资源开销和效率上却有特别的优势,较为适合在无线传感器网络中使用。Jiang 等人[9]引入双向散列链(dual directional hash chains, DDHC),保障组密钥的前向安全和后向安全,但其使用的是限时撤销策略,而且没有解决双向散列链固有特点带来的合谋攻击威胁。李林春等人[10]针对文献[9]的缺陷,提出适用于俘获攻击高发网络环境的组密钥管理方案,该方案还增加了合谋攻击的难度,但在网络环境极度恶劣的情况下资源开销会迅速增大。Dutta 等人[11]使用双向散列链,资源开销和效率都有较大的提高。杜春来等人[12]使用双向散列链,在不同会话使用独立的秘密多项式,建立成员节点秘密身份 ID,以秘密身份 ID 作为更新报文密钥素材提取参数。该方案可以实现节点的即时撤销,并能够大大降低节点资源开销。但文献[11,12]没有解决两个问题:a)如文献

收稿日期: 2012-01-12; **修回日期:** 2012-03-26 **基金项目:** 国家"973"计划资助项目(2011CB302906)

作者简介: 覃荣华(1985-),男,博士,主要研究方向为无线传感器网络密钥管理(qinronghua07@mails.gucas.ac.cn);何亮明(1984-),男,博士,主要研究方向为多媒体传感网信息处理;杨旭(1985-),男,硕士,主要研究方向为模式识别与信号处理;袁晓兵(1968-),男,研究员,博导,主要研究方向为通信与信息系统.

[10]所述,由于 DDHC 本身的固有特点,不能抵御合谋攻击;b)没有使用密钥缓冲链,不能实现组密钥的无缝切换。蔡云峰等人[13]对 DDHC 结构进行了改造,但其机制只能实现 δ 区间的合谋攻击抵制。

本文构建增强型双向散列链(EDDHC),提出基于 EDDHC 的自愈组密钥分发方法,有效地解决了基于传统双向散列链的组密钥分发方法对于妥协节点合谋攻击的安全性能问题,同时实现了组密钥的无缝切换和对发现的非法节点的即时撤销。

2　自愈组密钥分发方法模型

网络由组管理节点(group management sensor,GM)和组成员节点组成。GM 拥有较丰富的资源和处理能力,且安全可信。GM 主要负责组密钥管理保障组内通信安全、维护组内网络拓扑、数据融合、信息收集上报等。组成员节点资源受限,通信能力、存储能力和处理能力较差,负责数据的采集、处理和上报。把整个网络的生命周期分为 m 个会话阶段(session)。

为方便对方案功能模块和性能进行分析,下面以两个定义来对自愈组密钥分发方法模型进行诠释。

定义 1　有撤销能力的自愈组密钥分发方法满足:

a)组密钥按会话更新。

组内成员节点 $u_i \in G_j$,通过密钥更新包 B_j 及节点拥有的密钥素材 S_i 可以计算出 K_j,即满足关系

$$H(K_j \mid B_j, S_i) = 0 \tag{1}$$

另外,仅通过密钥更新包 B_j 或者节点密钥素材 S_i 是无法计算出 K_j,即满足关系

$$H(K_1, \cdots, K_m \mid B_1, \cdots, B_m) = H(K_1, \cdots, K_m \mid S_{G_1}, \cdots, S_{G_m}) = H(K_1, \cdots, K_m) \tag{2}$$

b)有 t-撤销能力是指所有被撤销节点的集合 $R = R_j \cup \cdots \cup R_1$,若 $|R| \leqslant t$,那么集合 R 节点通过所能获得的所有信息不能计算出 K_j,即

$$H(K_j \mid B_1, \cdots, B_j, S_R) = H(K_j) \tag{3}$$

c)所谓自愈是指成员节点 $u_i \in G_r$,在会话 r 到会话 s 间未被撤销,而正确接收到会话 B_r 和 B_s 后,即使 $B_x (r < x < s)$ 全部丢失的情况下,节点通过所能获得的信息可以恢复出 $K_x (r \leqslant x < s)$,即

$$H(K_r, \cdots, K_s \mid B_r, B_s, S_i) = 0 \tag{4}$$

定义 2　组密钥分发方法的前向安全、后向安全及合谋攻击抵制能力是:

a)前向安全。会话 j 前被撤销的节点集 $R \subseteq R_1 \cup, \cdots, \cup R_r$,通过它们自身可以获得的信息无法确定 K_j,即

$$H(K_j \mid B_1, \cdots, B_m, \{S_i\}_{u_i \in R}, K_1, \cdots, K_{j-1}) = H(K_j) \tag{5}$$

b)后向安全。会话 j 及以后加入组的节点集 $J \subseteq J_{j+1} \cup, \cdots, \cup J_m$,通过它们自身可以获得的信息无法确定 K_j,即

$$H(K_j \mid B_1, \cdots, B_m, \{S_i\}_{u_i \in J}, K_{j+1}, \cdots, K_m) = H(K_j) \tag{6}$$

c)合谋攻击抵制能力。会话 r 被剔除出组内通信的节点集 $C \subseteq R_r \cup, \cdots, \cup R_1$,以及在会话 s 后加入组的节点集 $D \subseteq J_s \cup, \cdots, \cup J_m$,若 $|C \cup D| \leqslant t$,这两个集合节点通过所能获得的所有信息仍然不能确定 $K_x (r \leqslant x < s)$,即

$$H(K_r, \cdots, K_{s-1} \mid B_1, \cdots, B_m, S_C, S_D) = H(K_r, \cdots, K_{s-1}) \tag{7}$$

3　增强型双向散列链(EDDHC)设计

对于 DDHC 结构,只需简单地反复迭代进行散列运算,已被撤销的节点可以计算出前向链 FHC 的后续会话序列值,新加入组的节点可以计算出后向链 BHC 的加入前会话的序列值。可见通过合谋攻击,完全可以对 DDHC 进行破解。本文方案特别针对 DDHC 的死肋进行结构性改造,解决合谋攻击抵制问题,以增强安全性能。

如图 1 所示,增强型双向散列链(EDDHC)由前向链 FHC、后向链 BHC、轻量级子链 LiBHC 和滑动窗口四个部分组成。满足以下条件:

$$\mathcal{H}(\mathrm{FHC}(j)) = \mathrm{FHC}(j+1) \tag{8}$$

$$\mathcal{H}(\mathrm{BHC}(j)) = \mathrm{BHC}(j-1) \tag{9}$$

$$\mathcal{H}_{\mathrm{light}}(\mathrm{LiBHC}(j)) = \mathrm{LiBHC}(j-1) \tag{10}$$

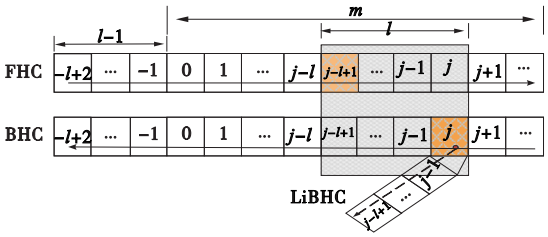

图1　增强型双向散列链结构(深色会话表示重构操作)

FHC 和 BHC 长度为 m,LiBHC 和滑动窗口长度为 l。滑动窗口是指 EDDHC 中以当前更新会话为起点,向后延伸 l 个会话区间产生的窗口。在有节点撤销行为的会话 j,以 $\mathcal{H}^{m-j}(s_{BS})$ 作为种子进行 $l-1$ 次反复散列 $\mathcal{H}_{\mathrm{light}}$ 运算,便可以得到会话 j 处的 LiBHC。因为 LiBHC 由 BHC 中有节点撤销行为的序列值作为种子生成得到,相对于 BHC 长度较短,故称为轻量级子链。若要进行节点撤销,会话 j 对应的滑动窗口的后向散列值以 LiBHC 代替,同时将 FHC$(j-l+1)$ 以一个新的随机数代替,导致 FHC 从会话 $j-l+1$ 开始被重构。这两步操作正是增强型双向散列链的精髓所在,它将改变密钥缓冲链中及后续使用的所有组密钥。

缓冲链滑动窗口$[j-l+1, j]$将当前会话 j 得到的 GK_j 置入缓冲链的链尾,即更新密钥放在滑动窗口的最右边,生效组密钥从窗口的最左边得到。缓冲链滑动窗口中丢失的密钥可以使用当前会话密钥更新信息和节点密钥素材通过自愈方式恢复。

下面论证 EDDHC 对合谋攻击的抵制能力。

命题 1　本方案针对双向散列链的固有特点,充分考虑组内出现合谋攻击对组密钥的安全威胁,使用 EDDHC 降低合谋攻击的可行性。

证明　EDDHC 有这样一个特点:在有节点撤销行为的会话 j,FHC 从 $j-l+1$ 开始自我重构,虽然不改动 BHC 的主链,却将滑动窗口左边$(l-1)$个会话的后向链序列值用 $\mathcal{H}^{m-j}(s_{BS})$ 作为种子的 LiBHC 链替换。GM 和成员节点中使用的组密钥缓冲链在有撤销行为的会话都将重新赋值,使得被撤销节点对组密钥缓冲链也没有可追溯知识。合谋攻击体现为利用先前会话 j_p 中被撤销的节点和当前会话 j_q 新加入节点所拥有的密钥素材知识总和,对 j_p 到 j_q 之间会话密钥的破解攻击。本方案 EDDHC 的自我重构行为使 j_p 被撤销节点的密钥素材知识无效化,即有

$$H(K_r, \cdots, K_{s-1} \mid B_1, \cdots, B_m, S_C, S_D) = H(K_r, \cdots, K_{s-1} \mid B_1, \cdots, B_m, S_D)$$

又因散列链的单向性,有

$$H(K_r,\cdots,K_{s-1}\mid B_1,\cdots,B_m,S_D)=H(K_r,\cdots,K_{s-1})$$

可见,EDDHC 降低了合谋攻击的可行性。证毕。

4 基于增强型双向散列链密钥分发方案

设节点集合为 $U=\{u_1,u_2,\cdots,u_n\}$。节点 u_i 生命周期对应于会话区间$[w,v]$。GM 和组成员节点都保留一个长度为 l 的组密钥缓冲链,并保存最新的前向散列值。表 1 是相关符号使用的描述。

表 1 符号表示

符号	意义
U	所有节点的集合
R	被撤销节点集合
U_{online}^{j}	会话 j 的在线成员节点集合
$\mathcal{H}$	单向散列函数,用于 FHC/BHC 的计算
$\mathcal{H}_{\text{light}}$	单向散列函数,用于 LiBHC 的计算
ID_i	节点 u_i 的秘密身份
S_i	节点 u_i 秘密多项式共享份额
$A_j(x)$	第 j 个会话广播更新包的访问多项式
$W_j(x)$	会话 j 的广播多项式
$B_j(x)$	会话 j 广播的组密钥更新包
GK_j	第 j 个会话更新的组密钥
GK_x^j	会话 j 处重构得到的用于替换 GK_x 的密钥
$\text{Enc}(X,h_j(\text{ID}_i))$	使用 $h_j(\text{ID}_i)$ 对 X 进行加密
D	当前会话与最近一个有节点撤销的会话的距离

1)系统建立

a)GM 选取有限域 F_q 中两个随机数 s_{FS} 和 s_{BS},用 s_{BS} 建立 BHC。选择 m 个独立的 c 阶多项式 $\{h_1(x),h_2(x),\cdots,h_m(x)\}$。

b)为请求加入的节点 $u_i\subset U$ 生成 ID_i,则 u_i 生命周期对应的 $S_i=\{h_1(\text{ID}_i),h_2(\text{ID}_i),\cdots,h_{1+v-w}(\text{ID}_i)\}$。

c)通过安全信道把 ID_i、S_i 和 $\text{FHC}(1-l)=\mathcal{H}(s_{FS})$ 发送给 u_i。安全信道是指 GM 与 u_i 之间的加密通信信道。

2)GM 广播组密钥更新包

a)若会话 j 不需要撤销节点,则更新 $\text{FHC}(j)=\mathcal{H}(\text{FHC}(j-1))$。若在会话 j 需要撤销节点,GM 首先需要更新 $\text{FHC}(j-l+1)=s_{FS\_new}$,其中 s_{FS_new} 为有限域 F_q 中的一个随机数。更新 $\text{FHC}(x)=\mathcal{H}^{x-(j-l+1)}(s_{FS\_new})$,$j-l+1\leqslant x$。用 $GK_x=\mathcal{H}_{\text{light}}^{j-x}(\mathcal{H}^{m-j}(s_{BS}))+\text{FHC}(x)$,$j-l<x<j$,代替组密钥缓冲链中对应位置的组密钥值。

b)计算并缓存 $GK_j=\mathcal{H}^{m-j}(s_{BS})+\text{FHC}(j)$。

c)随机选择混淆随机数 Z_j,计算 $A_j(x)=Z_j\prod_{u_i\subset U_{\text{online}}^{j}}(x-\text{ID}_i)+1$。

d)计算 $W_j(x)=A_j(x)\mathcal{H}^{m-j}(s_{BS})+h_j(x)$。

e)广播 $B_j(x)=\{R\}\cup\{W_j(x)\}$。

f)若会话 j 需要撤销节点,给在线成员节点发送对应的 $\text{Enc}(s_{FS\_new},h_j(\text{ID}_i))$。

3)组成员节点计算组密钥

a)组成员节点若没有被撤销并在生命周期内,在收到 GM 的广播 $W_j(x)$ 后,利用 $h_j(\text{ID}_i)\in S_i$,则有 $A_j(\text{ID}_i)=1$,计算 $\mathcal{H}^{m-j}(s_{BS})=W_j(\text{ID}_i)-h_j(\text{ID}_i)$。

b)验证 $\mathcal{H}[W_l(\text{ID}_i)-h_l(\text{ID}_i)]=\mathcal{H}^{m-l-1}(s_{BS})$ 是否成立。若成立,则接受 $\mathcal{H}^{m-j}(s_{BS})$,否则忽略 $B_j(x)$。

c)若会话 j 有撤销节点的行为,节点接收并解密 s_{FS_new},以 $GK_x=\mathcal{H}_{\text{light}}^{j-x}[\mathcal{H}^{m-j}(s_{BS})]+\mathcal{H}^{x-(j-l+1)}(s_{FS\_new})$ $(j-l+1\leqslant x\leqslant j)$ 代替原有组密钥缓冲链中对应位置的组密钥值,否则,将 $GK_j=\mathcal{H}^{m-j}(s_{BS})+\mathcal{H}(\text{FHC}(j-1))$ 插入密钥缓冲链。

4)组密钥的自愈

自愈操作按会话先后次序从前向后依次进行。生命周期为$[j_1,j_4]$的合法节点 u_i,当前组密钥滑动窗口为$[j-l+1,j]$,u_i 在会话 j 得到正确的 $\mathcal{H}^{m-j}(s_{BS})$,可以恢复在滑动窗口内会话 $j_2(j-l+1<j_2<j)$的组密钥。

a)检查会话区间$[j_2,j]$有无撤销节点行为。若没有,则 $\mathcal{H}^{m-j_2}(s_{BS})=\mathcal{H}^{j-j_2}[\mathcal{H}^{m-j}(s_{BS})]$,$\text{FHC}(j_2)=\mathcal{H}(\text{FHC}(j_2-1))$;若有,则找到滑动窗口中最后一个有撤销行为的会话 $j_3(j_2\leqslant j_3\leqslant j)$ 接收并解密 s_{FS_j3},得到 $h_{\text{BHC}}^{m-j_2}=\mathcal{H}_{\text{light}}^{j3-j_2}[\mathcal{H}^{m-j_3}(s_{BS})]$,另外有 $\text{FHC}(j_2)=\mathcal{H}^{j_2-j_3}(s_{FS\_j3})$。

b)计算 $GK_{j_2}=\mathcal{H}^{m-j_2}(s_{BS})+\text{FHC}(j_2)$ 或者 $GK_{j_2}^{j_3}=h_{\text{BHC}}^{m-j_2}+\text{FHC}(j_2)$。图 2 描述了没有节点撤销行为组密钥更新自愈的实现方式(有阴影的会话表示组密钥丢失,通过后续密钥更新报文自愈恢复);图 3 描述了在会话$(l+1)$有节点撤销行为组密钥更新自愈的实现方式。其中,URU 表示更新报文处理及节点撤销单元,GKG 表示组密钥生成模块,EK 为生效组密钥。

5)新节点的加入

a)节点 $u_{\text{new}}\in U'$在会话 j 请求加入组。

b)GM 为 u_{new}生成 ID_{new},与 u_{new}生命会话周期对应的 $S_{\text{new}}=\{h_j(\text{ID}_{\text{new}}),h_{j+1}(\text{ID}_{\text{new}}),\cdots,h_{j+v-w}(\text{ID}_{\text{new}})\}$,通过安全信道把 ID_{new}、S_{new}和 $\text{FHC}(j-l+1)$发送给 u_{new}。

c)u_{new}通过组密钥更新包 $B_j(x)$,以自愈方式可以生成组密钥缓冲链。

6)节点的撤销

a)在生命期区间外的会话 j 中,节点 u_i 无法计算出 GK_j,被强制排除出组内通信。

b)对于可疑恶意节点 u_{enemy},通过对组密钥更新包 $B_j(x)$ 中 $A_j(x)$的处理,使得 u_{enemy}计算出来的 $A_j(\text{ID}_{\text{enemy}})\neq 1$,从而得不到正确的 GK_j。

c)被撤销节点的 u_i 身份在 $B_j(x)$被公开,可以让组内成员节点对 u_i 进行隔离处理。

7)重新配置

成员节点 u_i 连续丢失多于 l 个会话的组密钥,这种情况下不能直接通过自愈方式得到恢复。从 GM 索取并解密 $\text{Enc}(\text{FHC}(j-l+1),h_j(\text{ID}_i))$后,才可以重新生成组密钥缓冲链。

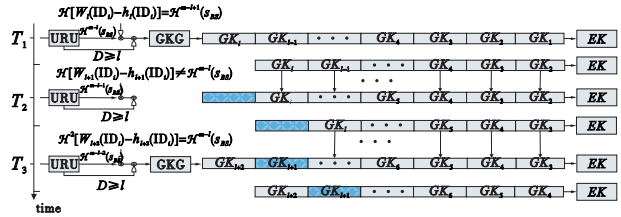

图2 没有节点撤销行为组密钥自愈方法

5 安全与效率分析

5.1 安全性分析

本方案使用增强型双向散列链结构,通过散列函数的单向性可以实现组密钥的认证,还可以保障组密钥的前向安全性和

后向安全性;使用节点的秘密身份来构造访问多项式,保障了节点身份的匿名性;组密钥的更新可以很方便安全地撤销非法节点。另外,本方案相比于文献[12],使用所提出的结合了 LiBHC 和密钥缓冲滑动窗口的 EDDHC 结构,可以抵御合谋攻击的威胁,更适用于俘获节点攻击高发的网络环境。

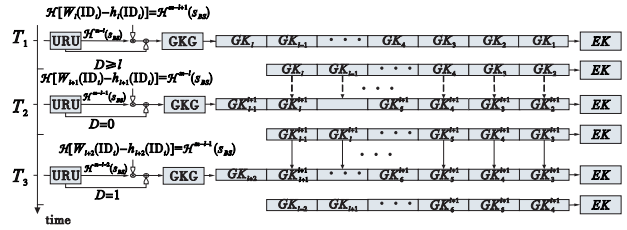

图3　有节点撤销行为组密钥自愈方法

5.2　效率分析

命题 2　本方案使用的组密钥缓冲链,可以实现组密钥使用的无缝切换。

证明　只要滑动窗口不连续丢失 l 个组密钥的更新信息,组密钥链总能进行自愈恢复先前丢失的组密钥。如图 2 所示,当前会话没有节点撤销行为,则组密钥直接通过双向散列链进行自愈;如图 3 所示,当前会话有节点撤销行为,则通过 LiBHC 和广播更新包中的前向链种子信息进行自愈。而且组内通信正在使用的生效组密钥取值于缓冲链滑动窗口最左边的组密钥值,滑动窗口中间会话组密钥的丢失并不影响通信数据包对组密钥的使用。换句话说,组密钥丢失会导致自愈行为,但不会影响组密钥使用的切换。证毕。

因为一方面,文献[12]的方案在效率上是基于 DDHC 方案,较具有代表性;文献[11]提供了三个策略:KD-1 使用向量空间方法,有较大的资源开销;KD-2 与文献[12]在性能和效率上基本一致;KD-3 安全性较差。另一方面,文献[10]只使用后向散列链,但其可以实现组密钥的无缝切换和提高合谋攻击难度,故本文只与文献[10,12]的方案进行效率对比。下面使用表 2 的变量符号,就本方案的资源开销进行具体分析。

表 2　变量的描述

变量符号	变量意义
p_r	滑动窗口中某个会话有撤销行为的概率
p_{com}	节点被攻击的概率
$p_{(L+F)}$	节点接收更新报文丢失的概率
$p_e(k)$	节点中滑动窗口缓冲链中出现 k 个空余单元
$\log q$	阶数为 q 的有限域占用的字长
T	撤销操作 $\text{Enc}(s_{FS\_new}, h_j(\text{ID}_i))$ 所占用的开销
R_{overhead}	$\{R\}$ 占用的通信开销(可以忽略不计[10])
E_{update}	节点组密钥更新信息包通信开销的期望
E_{rekey}	节点重新配置信息包通信开销的期望
$E_{\text{communication}}$	节点通信开销的期望

a)存储开销。本方案对组成员节点的存储开销为 $(v-w+l+3)\log q$ bit。其中包括对应于节点生命周期的 $(v-w+1)\log q$ 的秘密多项式 S_i、秘密身份 ID_i、长度为 l 组密钥链缓冲窗口以及与一个最新的前向链序列值。

b)通信开销。本方案的通信开销由组密钥更新信息开销 E_{update} 和重新配置信息开销 E_{rekey} 组成。那么有

$$p_e(k)=p_{(L+F)}^{(k)}(1-p_{(L+F)}) \quad k\leqslant l-2 \tag{11}$$

$$p_r=1-(1-p_{\text{com}})^t \tag{12}$$

$$E_{\text{update}}=(t+1)\log q+T+R_{\text{overhead}} \tag{13}$$

$$T=p_r\log q \tag{14}$$

$$E_{\text{rekey}}=p_{(L+F)}^{(l-1)}\log q \tag{15}$$

$$E_{\text{communication}}=E_{\text{update}}+E_{\text{rekey}} \tag{16}$$

使用节点总数为 2 000 个的网络,其生命周期分为 500 个会话数,多项式最大次数为 50,节点生命周期为 40 个会话数,节点被攻击的概率为 30%,丢包率为 30%,仿真分析相关开销及效率情况。图 4 显示了滑动窗口长度对 E_{update} 和 E_{rekey} 的影响。由图 4 可知,随着滑动窗口长度的变大,E_{update} 总体呈现上升趋势,而 E_{rekey} 则呈现下降趋势,且 E_{rekey} 相对于 E_{update} 几乎可以忽略不计。这是因为 E_{update} 中 T 随着窗口长度变大而变大,而 E_{rekey} 发生的概率较小,并随着窗口长度变大而迅速变小。

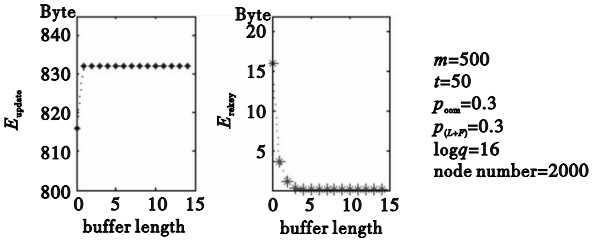

图4　通信开销中 E_{update} 和 E_{rekey} 与滑动窗口长度的关系

图 5 为本方案与文献[10,12]的节点通信开销的期望进行的对比,其中使用的滑动窗口长度为 6。由图 5 可见,文献[12]的 DDHC 方案 $E_{\text{communication}}$ 保持不变,而且是三者中最小的;文献[10]的方案在 p_{com} 较小时与 DDHC 方案很接近,但当 $p_{\text{com}}>0.9$ 时,随着 p_{com} 的增大,$E_{\text{communication}}$ 大幅度地上扬。EDDHC 方案比 DDHC 稍大,p_{com} 的增大对开销几乎没有什么影响。事实上,文献[10]方案在一些情况下需要进行全网的重新配置,整个网络的通信开销和 GM 的负担都将是难以忍受的。

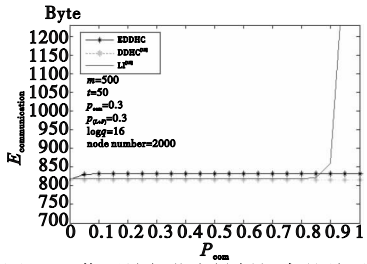

图5　通信开销与节点被俘概率的关系

c)计算开销。本方案的计算开销由处理 $W_j(x)$ 的有限域多项式乘法运算和散列运算组成。与文献[11,12]一样,本方案进行组密钥更新需要 $2(t+1)$ 次有限域乘法运算。滑动窗口的自愈操作只是增加了几次散列运算,散列运算在节点中远不会构成瓶颈。因此,本方案由于散列运算造成稍大的计算开销以获得更好的安全性能是可以接受的。

6　结束语

针对抵御合谋攻击的问题,本文提出一种基于增强型双向散列链具有撤销能力的自愈组密钥分发方案。在保持基于传统双向散列链自愈组密钥分发机制较好资源开销优势的前提下,获得更好的安全性和可靠性,更适用于节点俘获攻击高发、无线信道极不可靠的网络环境。

参考文献:

[1] STADDON J, MINER S, FRANKLIN M, *et al*. Self-healing key distribution with revocation[C]//Proc of IEEE Symposium on Security and Privacy. [S. 1.]: IEEE Press, 2002: 241-257.

(下转第 3474 页)

(上接第 3463 页)

[2] LIU Dong-gang, NING Peng, SUN Kun. Efficient self-healing group key distribution with revocation capability[C]//Proc of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003:231-240.

[3] BLUNDO C, D'ARCO P, De SANTIS A. On self-healing key distribution schemes[J]. IEEE Trans on information Theory, 2006, 52(12):5455-5467.

[4] DUTTA R, MUKHOPADHYAY S, DDOWLING T. Generalized self-healing key distribution in wireless Ad hoc networks with trade-offs in user's pre-arranged life cycle and collusion resistance[C]//Proc of the 5th ACM Symposium on QoS and Security for Wireless and Mobile Networks. New York: ACM Press, 2009:80-87.

[5] TIAN Bi-ming, HAN Song, DILLON T S. A self-healing key distribution scheme based on vector space secret sharing and one way hash chains[C]//Proc of International Symposium on a World of Wireless, Mobile and Multimedia Networks. Washington DC: IEEE Computer Society, 2008:1-6.

[6] TIAN Bi-ming, HAN Song, PARVIN S, *et al*. Self-healing key distribution schemes for wireless networks: a survey[J]. The Computer Journal, 2011, 54(4):549-569.

[7] PARK C, HUR J, KWEON K, *et al*. Self-healing key distribution scheme with long service time[J]. IEICE Electronics Express, 2010, 7(13):913-919.

[8] TIAN Bi-ming, HAN Song, DILLON T S. A self-healing and mutual-healing key distribution scheme based on bilinear pairings[C]//Proc of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. Washington DC: IEEE Computer Soiety, 2008:208-215.

[9] JIANG Yi-xin, LIN Chuang, SHI Ming-hui, *et al*. Self-healing group key distribution with time-limited node revocation for wireless sensor networks[J]. Ad Hoc Networks, 2007, 5(1):14-23.

[10] 李林春,李建华,潘军. 无线传感器网络中具有撤销功能的自愈组密钥管理方案[J]. 通信学报,2009,30(12):12-17.

[11] DUTTA R, MUKHOPADHYAY S, COLLIER M. Computationally secure self-healing key distribution with revocation in wireless and Ad hoc networks[J]. Ad Hoc Networks, 2010, 8(1):597-613.

[12] 杜春来,胡铭曾,张宏莉,等. 基于双向散列链具有撤销能力的自愈组密钥分发机制[J]. 通信学报,2009,30(6):33-37.

[13] 蔡云峰,毛宇光. 无线传感器网络中滑动窗口自愈的密钥分发机制[J]. 计算机应用研究,2011,28(1):338-340.