无线传感器网络中自修复密钥颁布机制中滑动窗口的动态性探讨

孙新江,吴晓蓓,黄 成,徐志良
(南京理工大学自动化学院,江苏南京 210094)

摘 要: 在很多自修复密钥颁布机制中,滑动窗口大小影响着密钥的修复性能和通信开销.本文利用概率知识,首次建立了滑动窗口和丢包率对节点密钥同步性能、组安全关联性能和安全服务性能的数学模型.设计了适应链路动态变化特性的滑动窗口选择机制,采用查找表方式优化了计算和存储开销.仿真验证了该机制具有动态适应性,可以高概率的保证网络的安全服务性能.与已有机制相比,所提机制显著降低了通信开销,具有可行性和高效性,进一步推动了自修复密钥颁布机制的实际应用.

关键词: 无线传感器网络; 自修复密钥颁布; 滑动窗口; 动态链路; 丢包率; 自适应
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2015)03-0447-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.03.005

Exploring the Dynamic of Sliding Window for Self-Healing Key Distribution Schemes in Wireless Sensor Networks

SUN Xin-jiang, WU Xiao-bei, HUANG Cheng, XU Zhi-liang
(*School of Automation, Nanjing University of Science and Technology, Nanjing, Jiangsu* 210094, *China*)

Abstract: In many self-healing key distribution schemes, the size of sliding window affects both the self-healing capability and the communication overhead. With probability knowledge, the mathematical model is built, which reflects the influence of the size of sliding-window and packet loss rate on the performance of key synchronization, group security association and security service. Then, an adjustment mechanism of sliding window is proposed to adapt to the dynamic change of broadcast links, and a look-up table is utilized to reduce the computation and storage overhead. Simulation results show that the scheme proposed is dynamically adaptive, and guarantees the performance of security service with high probability. Compared with the existing schemes, the proposed scheme greatly reduces the communication overhead, and is more feasible and efficient. Meanwhile, it further promotes the application of self-healing key distribution.

Key words: wireless sensor networks; self-healing key distribution; sliding window; dynamic links; packet loss rate; self-adaptive

1 引言

无线传感器网络(WSNs)在一些环境恶劣的军事战场或者商业应用中,会面对一些潜在的攻击威胁,这就要求在WSNs协议设计中必须仔细地考虑安全问题,用来抵挡恶意入侵、攻击[1].密钥管理以实现网内不同节点密钥信息的颁发和维护,建立起节点之间的安全关联[2],是WSNs中安全通信机制的核心技术.

由于实际拓扑变化、环境变化以及人为干扰等造成链路中随机性丢包错包现象,颁布密钥的广播消息不能够被网内节点以100%的概率接收到,造成密钥更新失败、密钥不同步乃至安全关联失败的现象.如何实现在不可靠链路下密钥的颁布与维护,是近几年的研究热点[3].文献[4]首次给出了自修复密钥颁布机制,在广播消息中添加一些冗余信息,使节点可以无需与组管理者进行交互而自主地恢复之前丢失的密钥,实现了对链路丢包的容忍.目前根据冗余信息的构造方法,密钥的自修复分为相关联修复和独立修复[3].相关联修复方法[5~9]具有较小的通信开销,但是存在着一些问题[3],如后向安全性,合谋攻击的弱抵抗,节点不能被任意撤

收稿日期:2013-09-27;修回日期:2014-02-09;责任编辑:覃怀银
基金项目:教育部博士点专项目基金咨助项目(No.20113219110028);江苏省自然科学基金资助项目(No.BK2012803)

销,支持密钥更新次数有限以及计算复杂度较高等.独立修复方法可避免前者存在的一些问题[3],但在恢复同样数目的密钥时产生更大的通信开销,见表 1.文献[10]指出已有的自修复机制因通信开销过大而不具有实际应用的可行性.考虑到网络链路随机故障时连续丢失密钥消息的数目不会太长,文献[11]提出了 δ 滑动窗口机制,只要节点不连续丢失 δ 个密钥消息,就可修复失去的密钥.文献[12~14]设计了类似机制,来减小通信开销.但是,上述自修复机制[11~14]中均采用固定窗口,事实上,过大的窗口会造成通信资源的浪费,过小则使节点无法恢复出丢失的密钥而脱离网络.

表 1 几种独立自修复方法的通信开销

机制	通信开销($\log_2 q$)	机制	通信开销($\log_2 q$)
Liu et al.'s sch3[12]	$(m+j+1)t+m+1$	Blundo et al.'s sch3[15]	$(2t+1)j$
Hong et al.'s sch2[16]	$(t+1)j+\sum_{i=1}^{j}\mid R_i\mid$	Dutta et al.'s[17]	$t+j+1$
Wang et al.'s[18]	$2j+\sum_{i=1}^{j}(\max\{t,\mid G_j\mid+1\})$	Wang et al.'s[19]	$(t+1)v+j$
More et al.s[11]	$3t^2+(5+8\delta)t+4\delta+1$	Han et al.'s[13]	δt

注:q 为一大素数,δ 为滑动窗口大小,m 为支持的最大密钥更新次数,j 为当前密钥更新编号,t 为秘密共享多项式的阶次,R_i 为第 i 次密钥更新时被撤销的节点集合,满足 $1\leq i\leq j$,v 为前 j 次密钥更新时新节点加入的个数,满足 $0\leq v\leq j\leq m$

针对以上问题并从网络的实际应用出发,本文首先定义了自修复密钥颁布机制的安全性指标,如节点密钥同步、安全关联以及安全服务性能;然后分析并建立了广播链路的丢包率和滑动窗口对网络安全性能的概率数学模型;接着给出滑动窗口的动态选择机制,以适应链路的不可靠性;采用查找表法进行优化,减少计算和存储开销.仿真验证了提出机制的高效性和可行性,能以高概率保证网络安全服务性能;通过与已有机制相比,明显降低了通信开销.

2 网络假设与安全性能定义

2.1 概率知识

考虑 n 次独立不相关的伯努利实验.设 p 为一次实验的成功概率,q 为失败概率,$p+q=1$,且 $0<p,q<1$.本文将出现连续至少 k 次失败的情况定义为绝对失败,$1<k\leqslant n$.文献[20]给出了 n 次实验中出现连续失败次数的最大值 L_n 的概率分布为

$$P(L_n=k)=q^n\sum_{y=\lfloor n/(k+1)\rfloor}^{n-k}(p/q)^y\cdot \sum_{i=1}^{y+1}\binom{y+1}{i}C(n-y-ik,y+1-i,k-1) \quad (1)$$

其中

$$C(\alpha,r,k)=\begin{cases}\sum_{j=0}^{r}(-1)^j\binom{r}{j}\binom{\alpha-(k+1)j+r-1}{r-1}, & \text{if } \alpha>0\\ 1, & \text{if } \alpha=0\\ 0, & \text{otherwise}\end{cases} \quad (2)$$

出现连续失败次数 L_n 至少为 k 的概率为

$$P(L_n\geq k)=\sum_{m=k}^{n}P(L_n=m)=q^n\sum_{m=k}^{n}\sum_{y=\lfloor n/(m+1)\rfloor}^{n-m}(p/q)^y\cdot\sum_{i=1}^{y+1}\binom{y+1}{i}C(n-y-im,y+1-i,k-1) \quad (3)$$

文献[21]给出了另外一种简洁的表达式

$$P(L_n\geq k)=\sum_{m=1}^{\lfloor\frac{n+1}{k+1}\rfloor}(-1)^{m-1}q^{mk}p^{m-1}\left(\binom{n-mk}{m-1}+p\binom{n-mk}{m}\right) \quad (4)$$

考虑 N 组实验同时进行,每组实验进行 n 次,则最多有 M 组出现绝对失败的概率为

$$P_N^M=\sum_{i=0}^{M}C_i^N(P(L_n\geq k))^i(1-P(L_n\geq k))^{N-i} \quad (5)$$

其中 $0\leqslant M\leqslant N$.

2.2 网络假设

在实际应用中,面对实时网络任务,可将网内不同区域或功能的节点进行分组,以提高管理的灵活性和扩展性.本文采用常见的组通信网络模型[3],组内均有至少一个资源较丰富(能量、计算、存储)的高能节点和若干个一般节点.高能节点作为组管理 GM,与基站直接通信,负责组内安全管理功能,如密钥颁布、维护以及入侵检测等;而一般节点为组内成员 SN_i($i=1,2,\cdots,N$,N 为组内节点总数),接收密钥更新消息,完成数据感知和安全传输等功能.为保证安全通信,GM 会定期广播密钥更新消息,SN_i 更新并修复丢失的密钥信息.

2.3 安全性能定义

定义 1 密钥同步性能 是指组内节点与组管理者的密钥同步性能,用节点获得的组密钥与当前组管理者颁布的组密钥的版本之差来度量,记为 SycK_i,$i=$

$1,2,\cdots,N$.

当 $\mathrm{SycK}_i = 0$ 时,节点达到密钥绝对同步;SycK_i 越大,节点的密钥同步性能就越差;当 $\mathrm{SycK}_i > \delta$,认为该节点 i 失去了密钥同步的机会,出现密钥同步失败,其中 δ 为滑动窗口大小.由于密钥的动态自修复,节点的密钥同步性能具有动态变化的特点.

定义 2　安全关联性能　是指组内节点在一次密钥消息广播后,获得与 GM 以及其他成员之间密钥的一致性,用当前组内达到密钥绝对同步的节点所占比例来度量,记为 SA.

SA 反映了当前密钥消息广播后组内可用节点的百分比,其值越大表明有越多的可用节点与 GM 进行安全通信.

定义 3　安全服务性能　是指特定的一段时间(密钥更新次数)内在不可靠链路下组内节点始终维持密钥同步性的能力,用维持密钥同步的节点所占百分比来度量,记为 σ.

安全服务指标 σ 反映的是一段时间组内始终可用的节点数目,即组内执行任务能力的大小.σ 越大,说明有越多的节点可以安全地服务于网络任务;反之,网络的安全服务能力越差.

3　滑动窗口的自适应选择机制

3.1　节点的密钥同步性能

假设一次密钥广播消息有 λ 个数据包,GM 与节点 i 的链路丢包率为 p_e^i,那么节点 i 接收密钥消息失败的概率为

$$P_e^i = 1 - (1 - p_e^i)^{\lambda} \tag{6}$$

由式(4)可得,连续丢失密钥消息次数至少为 $\delta+1$ 次,即节点出现密钥同步失败的概率为

$$\begin{aligned} P_e^{i,\delta} &= P(\mathrm{SycK}_i \geq \delta + 1) \\ &= \sum_{m=1}^{\lfloor \frac{n+1}{\delta+2} \rfloor} (-1)^{m-1} (P_e^i)^{m(\delta+1)} (1 - P_e^i)^{m-1} \\ &\cdot \left(\binom{n - m(\delta+1)}{m-1} + (1 - P_e^i) \binom{n - m(\delta+1)}{m} \right) \end{aligned} \tag{7}$$

图 1 给出了在密钥消息广播 $n = 50$ 次后节点出现密钥同步失败的概率随着不同丢包率和滑动窗口的变化曲线(不失一般性,考虑一次密钥消息的最大长度 1440bytes 以及 tinyos 中数据包的最大载荷 36bytes[10],则每次广播包含的数据包最多有 $\lambda = 40$).可以看出,节点出现密钥同步失败的概率随着 δ 的增大和 p_e^i 的减小而减小.

3.2　网络的安全关联和服务性能

考虑组内有 N 条链路广播,每条链路的丢包率为 $p_e^i, i = 1,2,\cdots,N$.为简化处理,假设每条链路的丢包率均为 p_e.由式(6)可得,第 j 次密钥颁布后组内安全关联 $SA_j = \eta (0 \leqslant \eta \leqslant 100\%)$ 的概率为

$$\begin{cases} P_e = 1 - (1 - p_e)^{\lambda} \\ P(\mathrm{SA}_j = \eta) = \sum_{i=0}^{\lceil \eta N - Nd_j \rceil} C_i^N (1 - P_e)^i (P_e)^{N-i} \end{cases} \tag{8}$$

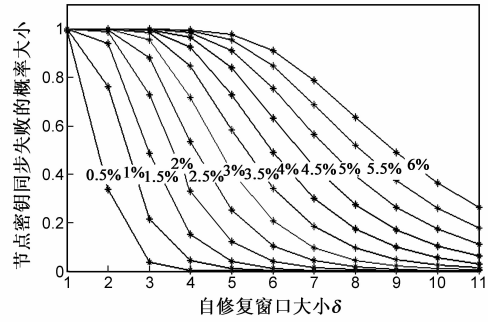


图1　在不同丢包率下节点出现密钥同步失败的概率随着滑动窗口的变化曲线

其中 Nd_j 为前 j 次密钥颁布中组内已出现密钥同步失败的节点数目.

由式(6)~(8),最少有 σN 条链路在 n 次广播通信中始终维持密钥同步的概率 $P_N^{\delta,\sigma} (0 \leqslant \sigma \leqslant 100\%)$ 为

$$\begin{cases} P_e = 1 - P_s = 1 - (1 - p_e)^{\lambda} \\ P_e^{\delta} = \sum_{m=1}^{\lfloor \frac{n+1}{\delta+2} \rfloor} (-1)^{m-1} (p_e)^{m(\delta+1)} (1 - p_e)^{m-1} \\ \cdot \left(\binom{n - m(\delta+1)}{m-1} + (1 - p_e) \binom{n - m(\delta+1)}{m} \right) \\ P_N^{\delta,\sigma} = \sum_{i=0}^{\lfloor (1-\sigma)N \rfloor} C_i^N (P_e^{\delta})^i (1 - P_e^{\delta})^{N-i} \end{cases} \tag{9}$$

图 2 给出在不同丢包率 p_e 下,在 $N = 50$ 中 $n = 50$ 次广播通信[10]中组内有至少 $\sigma = 98\%$ 的节点始终够维持密钥同步的概率 $P_N^{\delta,\sigma}$ 随 δ 的变化曲线.可知,$P_N^{\delta,\sigma}$ 随着 p_e 的增大而减小,同时随着 δ 的增大而渐近地接近 1.

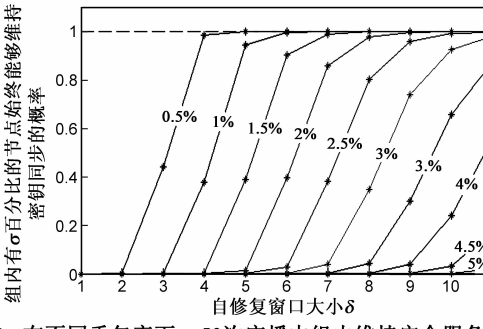


图2　在不同丢包率下n=50次广播中组内维持安全服务指标σ=98%的概率P_N^{σ}随着σ的变化曲线

3.3 滑动窗口的动态选择

3.3.1 设计目标

假设组内有 N 个$SN_i, i=1,2,\cdots,N$ 和 1 个组 GM. 在执行一次网络任务的过程中,预计组内需要 n 次广播通信来更新组密钥,以确保安全通信.由于节点部署的冗余性,在任务执行过程中需要以不低于 $\tilde{P}_N^{\sigma}$ 的概率保证指标 σ,即有 σ 比重的节点能够始终安全地服务于任务需求,同时尽量减小节点资源开销.

3.3.2 设计方法

假设每 Δ_0 次广播通信后,组管理者依据当前评估的广播链路丢包率的最大值 $p_{e,\max}=\max\{p_e^i\}_{i=1,2,\cdots,N}$、一次密钥广播消息中包含的数据包个数 λ 和 σ 以及目标概率 $\tilde{P}_N^{\sigma}$,通过建立的概率模型得到最优的滑动窗口值 δ_{opt}. Δ_0 的值取决于广播链路的动态变化特性,链路变化越频繁,Δ_0 取值越小,同时满足 $1\leqslant\Delta_0\leqslant n$.针对不同的应用,可以选取不同的 λ、Δ_0、N 和 $\tilde{P}_N^{\sigma}$,建立模型 $\delta_{opt}=F(p_{e,\max},\lambda,\Delta_0,N,\sigma,\tilde{P}_N^{\sigma})$.在实际操作中可根据实时评估的 $p_{e,\max}$,来获得 δ_{opt}.算法流程见算法 1.

算法 1 组密钥自修复中动态窗口计算

输入: $\lambda,\Delta_0,N,n,\sigma$ 和 $\tilde{P}_N^{\sigma}$
输出: δ_{new}

```
for i = 1 to n do
    if i++ mod Δ0 == 0 do
        评估当前各广播链路的丢包率 p_e^i, i = 1,2,…,N;
        得丢包率的最大值 p_{e,max} = max{p_e^i}_{i=1,2,…,N}
        由参数输入和 p_{e,max},利用式(9)的模型,得到最优的窗口大
        小 δ_new = F(p_{e,max},λ,Δ0,N,σ,P̃_N^σ):
        用 δ_new更新当前的 δ;
    else
        维持旧的窗口 δ;
    end if
end for
```

3.3.3 广播链路丢包率的评估

由于提出的机制是建立在丢包率的预测、评估之上的,丢包率的准确性直接影响着机制的可用性.文献[22]给出了分析和评价数据包丢失过程的马尔科夫模型;文献[23]给出了丢包率的预测模型,可快速、准确地预测丢包率;文献[24]从实际应用的角度,能测得链路质量因子 LQI 与数据包重传次数(丢包率)的关系.本文主要致力于基于丢包率的滑动窗口选择机制的设计,丢包率的评估和预测不在本文的讨论范围之内.

3.3.4 滑动窗口的最优解

针对式(9)中 δ_{opt}与 p_e,λ,n,N,σ 和 $\tilde{P}_N^{\sigma}$ 之间非线性关系的解析解很难得到的问题,本文将其转化为下面非线性的优化问题

$$\min\{\delta\}$$

$$\text{s.t.}\begin{cases} P_e=1-(1-p_{e,\max})^{\lambda} \\ P_e^{\delta}=\sum\limits_{m=1}^{\lfloor\frac{n+1}{\delta+2}\rfloor}(-1)^{m-1}(P_e)^{m(\delta+1)}(1-P_e)^{m-1}\cdot \\ \left(\binom{\Delta_0-m(\delta+1)}{m-1}+(1-P_e)\binom{\Delta_0-m(\delta+1)}{m}\right) \\ P_N^{\delta,\sigma}=\sum\limits_{i=0}^{\lfloor(1-\sigma)N\rfloor}C_i^N(P_e^{\delta})^i(1-P_e^{\delta})^{N-i} \\ P_N^{\delta,\sigma}\geqslant\tilde{P}_N^{\delta,\sigma} \\ \delta\in Z_+ \end{cases} \tag{10}$$

由于迭代运算需要大量计算开销,上述优化问题在有限时间内不能保证得到最优解,同时不同的丢包率需要重复计算,所以该方法不适合节点资源受限以及实时性要求的场合.

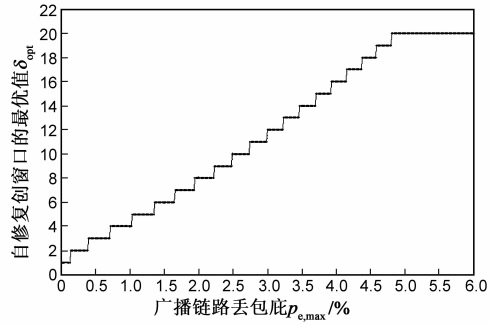


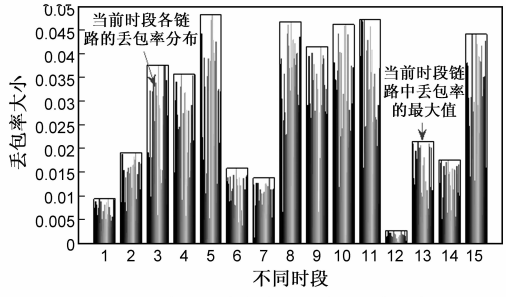
图3 在网络参数N=50,σ=90%,$\tilde{P}_N^{\sigma}$=90%,λ=40,Δ_0=20下滑动窗口δ_{opt}随丢包率$p_{e,max}$的变化曲线

为了解决实时性要求,这里采用查表方法,预先计算并存储一组 δ_{opt}和丢包率 $p_{e,\max}$的数据曲线关系,根据丢包率的情况,实时地直接查找 δ_{opt}.下面以一例来说明基于查表的自修复窗口动态选择过程.不失一般性[10],假设组内有 $N=50$ 个普通节点来完成某一数据采集或控制的任务,一次密钥消息中数据包最多为 $\lambda=40$ 个,通过选择 δ_{opt}来实现在 $\Delta_0=20$ 次密钥颁布过程中以概率 $\tilde{P}_N^{\sigma}=90\%$ 保证安全服务指标 $\sigma=90\%$.图 3 给出了 δ_{opt}随 $p_{e,\max}$的变化曲线.可见,滑动窗口的最优解随丢包率呈分段变化,即在局部每段丢包率范围内最优的滑动窗口值是固定的.组管理者存储相应的分段关系,就可根据实时的丢包率来获得最优解,这样处理大大减小了计算和存储开销.

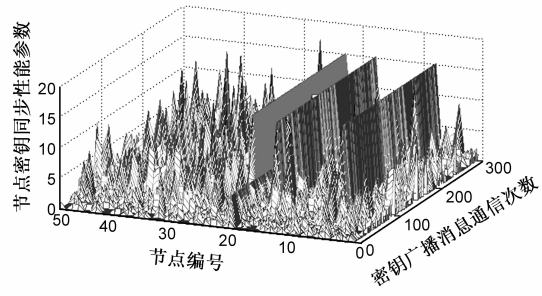
4 仿真与结果分析

本文利用 matlab 工具设计了无线传感器网络的组通信场景[3].假设组内有 50 个组成员,一次密钥广播消息中包含 40 个数据包,在 300 次广播通信中以 90% 的

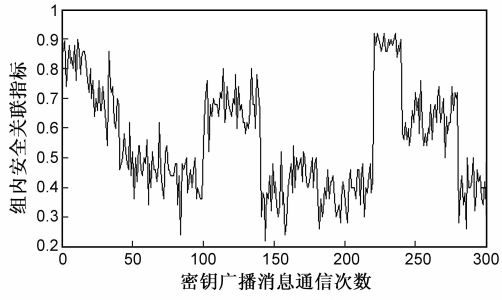
概率实现组内有 90% 的节点始终能够安全地服务于网络任务,即 $N=50,\sigma=90\%,\tilde{P}_N^{\sigma}=90\%,\lambda=40,\Delta_0=20,n=300$.另外,组内 50 个广播链路在 $n/\Delta_0=15$ 个时段内随机赋予在 5% 范围内的丢包率.组管理者离线计算并存储当前系统参数下滑动窗口的最优值随丢包率的变化曲线,见图 3.



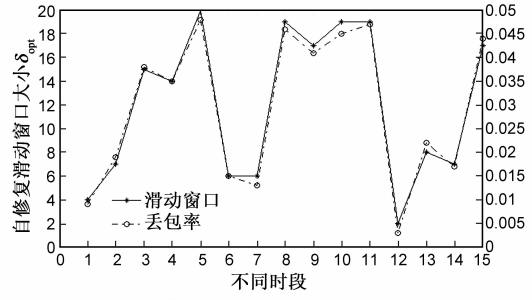
(*a*) 各时段中各广播链路丢包率分布



(*b*) 各个节点的密钥同步性能参数分布



(*c*) 组内安全关联指标



(*d*) 最优滑动窗口随丢包率变化关系

图4　仿真试验结果

图 4 给出了一次仿真试验结果.由图 4(*a*)可以看到同一时段内不同链路的丢包率是不同的,在不同时段内最大丢包率也是不同的.图 4(*b*)表明有 4 个节点出现密钥同步失败,即组内安全服务参数为 $\hat{\sigma}=(N-4)/N\times100\%=92\%$,比目标值 $\sigma=90\%$ 还要高.图 4(*c*)对比图 4(*a*),可以发现安全关联指标与丢包率成反比,丢包率越高,其安全关联指标越低.在安全关联参数动态变化降到在 25% 左右时,即有 75% 的节点链路出现了丢包现象,节点的密钥同步性能由于自修复而得到动态的改善,最终整个过程中有 92% 的节点能够安全地服务于网络任务.图 4(*d*)图说明了最优滑动窗口随不同丢包率的一致性变化.

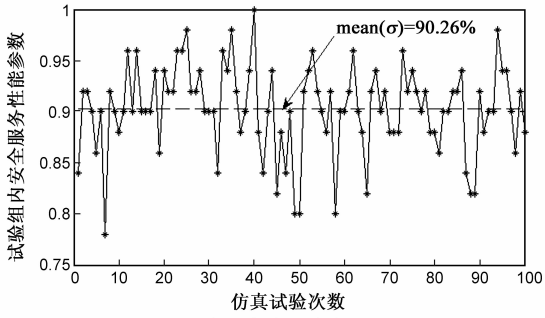


图5　100次试验组安全服务性能的分布图

图 5 给出了经过 100 次试验后得到的组安全服务性能的分布图.可以看出,基于概率模型的滑动窗口自适应选择机制虽然每次试验的安全服务性能不完全相同,但所有试验结果的平均安全服务性能 $\bar{\sigma}=90.26\%$,大于目标性能参数 90%.本文将小于目标值 $\sigma=90\%$ 的实验结果定义为出现误差,即 $e_i=\sigma-\sigma_i$,每次误差出现的概率为 $\frac{1}{T}$,其中 σ_i 为第 i 次试验结果的安全服务指标,$i=1,2,\cdots,T$,T 为试验次数.通过分析计算,可以得到上述方法的平均误差和标准残差分别为

$$\bar{e}=\sum_{i=1}^{T}\frac{1}{T}e_i=0.0146,\sigma_e=\sqrt{\frac{1}{T}\sum_{i=1}^{T}e_i^{\,2}}=9.96\times10^{-4}.$$

这说明了本文所设计的机制在统计意义上能够以具有足够小的误差来保证目标安全服务指标.

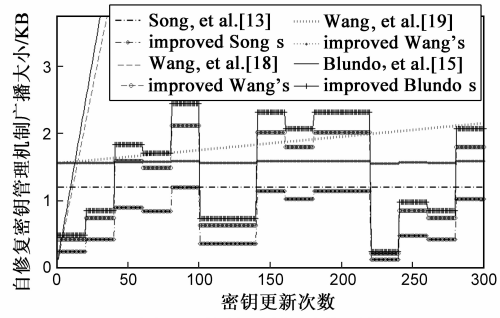


图6　不同机制的通信开销

不失一般性,选取:$t=30,\log_2 q=16,G_i=50,R_i=$

$0, m = 50, v = 0.5\text{m}, i = 1, 2, \cdots, 300$,用于表 1 所列方法中.图 6 给出了在相同条件下已有典型机制及其基于动态自修复窗口的改进机制中密钥广播消息长度随密钥广播次数 j 的变化曲线.可看出,已有机制[13,15,18,19]采用本文设计的动态窗口机制进行优化,可以显著减小密钥广播消息的长度.相比固定的滑动窗口[13],可以减小至少 40% 的通信开销.

5 总结与展望

本文设计的滑动窗口自适应选择机制可以应用于几乎所有的独立自修复密钥颁布机制[11~13,15~19],能够对动态链路具有适应性,以高概率和低误差保证网络的安全服务性能,具有高效性和可行性.丢包率的准确性评估和结合其他因素来提高网内安全服务性能的保证概率,是自修复密钥颁布机制研究的方向.

参考文献

[1] CHEN X Q, MAKKI K, et al. Sensor network security: A Survey[J]. IEEE Communications Surveys & Tutorials, 2009, 11(2): 52 – 73.

[2] ZHANG J Q, VARADHARAJAN V. Wireless sensor network key management survey and taxonomy[J]. Journal of Network and Computer Applications, 2010, 33(2): 63 – 75.

[3] RAMS T, PACYNA P. A survey of group key distribution schemes with self-healing property[J]. IEEE Communications Surveys & Tutorials, 2013, 15(2): 820 – 842.

[4] STADDON J, MINER S, et al. Self-healing key distribution with revocation[A]. Proceedings of IEEE Symposium on Security and Privacy [C]. Los Alamitos: IEEE Press, 2002. 241 – 257.

[5] DUTTA R, MUKHOPADHYAY S, et al. Computationally secure self-healing key distribution with revocation in wireless ad hoc networks[J]. Ad Hoc Networks, 2010, 8(6): 597 – 613.

[6] 彭清泉,裴庆祺,等.无线传感器网络中自治愈的群组密钥管理方案[J].电子学报,2010,38(1):123 – 128.
PENG Qing-quan, PEI Qing-qi, et al. A self-healing group key management scheme in wireless sensor networks[J]. Acta Electronica Sinica, 2010, 38(1): 123 – 128. (in Chinese)

[7] DUTTA R, SANYAL S. Collusion resistant selfhealing key distribution in mobile wireless networks[J]. International Journal of Wireless and Mobile Computing, 2012, 5(3): 228 – 243.

[8] JIANG Y X, LIN C, 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.

[9] 王顺满,陶然,等.具有自我恢复功能的密钥管理方法在 MANET 网络中应用研究[J].电子学报,2009,37(4):889 – 893.
WANG Shun-man, TAO Ran, et al. Research of the self-healing key management in MANET[J]. Acta Electronica Sinica, 2009, 37(4): 889 – 893. (in Chinese)

[10] WANG Q H. Practicality analysis of the self-healing group key distribution schemes for resource-constricted wireless sensor networks[A]. Proceedings of the 3rd IEEE International Conference on Communications and Mobile Computing[C]. Piscataway: IEEE, 2011. 37 – 40.

[11] MORE S M, MALKIN M, et al. Sliding-window self-healing key distribution[A]. Proceedings of the 10th ACM Conference on Computer and Communications Security[C]. New York: ACM, 2003. 82 – 90.

[12] LIU D, NING P, et al. 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.

[13] HAN S, TIAN B M, et al. Efficient threshold self-healing key distribution with sponsorization for infrastructureless wireless networks[J]. IEEE Transactions on Wireless Communications, 2009, 8(4): 1876 – 1887.

[14] 杜春来,胡铭曾,等.基于滑动窗口的移动自组网的自愈密钥发布机制[J].通信学报,2009,30(2):6 – 11.
DU Chun-lai, HU Ming-zeng, et al. Self-healing key distribution scheme of MANET based on sliding window[J]. Journal on Communications, 2009, 30(2): 6 – 11. (in Chinese)

[15] BLUNDO C, et al. Design of self-healing key distribution schemes[J]. Designs, Codes and Cryptography, 2004, 32(1 – 3): 15 – 44.

[16] HONG D W, Kang J S, et al. An efficient key distribution scheme with self-healing property[J]. IEEE Communications Letters, 2005, 9(8): 759 – 761.

[17] DUTTA R, WU Y D, et al. Constant storage self-healing key distribution with revocation in wireless sensor network[A]. Proceedings of 2007 IEEE International Conference on Communications[C]. Piscataway: IEEE, 2007. 1323 – 1328.

[18] WANG Q H, CHEN H F, et al. Access-polynomial-based self-healing group key distribution scheme for resource-constrained wireless networks[J]. Security and Communication Networks, 2012, 5(12): 363 – 1374.

[19] WANG Q H, CHEN H F, et al. One-way hash chain-based self-healing group key distribution scheme with collusion resistance capability in wireless sensor networks[J]. Ad Hoc Networks, 2013, 11(8): 2500 – 2511.

[20] MAKRI F S, Philippou A N, et al. Shortest and longest length of success runs in binary sequences[J]. Journal of Statistical Planning and Inference, 2007, 137(7): 2226 – 2239.

[21] MUSELLI M. Simple expressions for success run distributions in Bernoulli trials[J]. Statistics & Probability Letters, 1996, 31(2): 121 – 128.

[22] MARTINEZ G E, et al. Modeling and analysis of the packet-

level loss process in wireless channels[A]. Proceedings of the 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems[C]. New York: ACM, 2010. 283 – 290.

[23] LIU F Q, LIN C. An analytical method to predict packet losses over bursty wireless channels[J]. IEEE Communications Letters, 2011, 15(12): 1338 – 1340.

[24] RAMALINGAM K C, et al. SIMAGE: secure and link-quality cognizant image distribution for wireless sensor networks. 2012 IEEE Global Communications Conference[C]. Piscataway: IEEE, 2012. 616 – 621.

作者简介

孙新江　男,1989 年 5 月出生于河南三门峡.博士研究生.主要研究方向为无线传感器网络安全、多源协作网络编码及其安全.
E-mail: xinjiangsun@gmail.com

黄　成　男,1975 年 7 月出生于江苏南通.博士研究生,讲师.主要研究方向为无线传感器网络、自动化检测技术.
E-mail: hearthc@163.com

吴晓蓓(通信作者)　女,1958 年 8 月出生于四川成都.教授,博士生导师.主要研究方向为无线传感器网络、智能控制.曾获得部省级科技进步二等奖和三等奖;获国家教学成果一、二等奖;国家级教学名师;发表论文 80 余篇等.
E-mail: wuxb@njust.edu.cn

徐志良　男,1962 年 9 月出生于浙江宁波.教授,硕士生导师.主要研究方向为为自动检测理论与技术、智能传感器与网络化技术.
E-mail: hearthc@163.com