第 35 卷 第 11 期 计 算 机 工 程 2009 年 6 月
Vol.35 No.11 Computer Engineering June 2009
·安全技术· 文章编号：1000—3428(2009)11—0152—03 文献标识码：A 中图分类号：TP393

无线传感器网络中的多次密钥协商

孙发军[1]，周志强[1]，张 文[2]
(1. 怀化学院数学与应用数学系，怀化 418008；2. 怀化学院计算机科学与技术系，怀化 418008)

摘 要：无线传感器网络链路损耗大，需要进行多次密钥协商。为研究增加密钥协商次数对提高网络安全连通率的效力，引入加权安全连通率和性价比(CPR)2 个指标，并在 TOSSIM 平台上进行仿真验证。CPR 随协商次数的增加而降低，仿真结果及理论分析表明，为获得较高安全连通率，重复协商次数取 3~4 较合适。

关键词：无线传感器网络；密钥管理；安全连接；安全连通性；性价比

Repetitious Key Negotiations in Wireless Sensor Networks

SUN Fa-jun[1], ZHOU Zhi-qiang[1], ZHANG Wen[2]
(1. Department of Mathematics and Applied Mathematics, Huaihua University, Huaihua 418008;
2. Department of Computer Science and Technology, Huaihua University, Huaihua 418008)

【Abstract】Key negotiation needs several times in Wireless Sensor Networks(WSN) because of high loss rate. In order to research the effectiveness of repetitious key negotiations on heightening secure connectivity, it proposes two metrics named the weighing secure connectivity and Cost Performance Ratio(CPR), and it processes the simulation experiments on TOSSIM platform. CPR becomes lower and lower as the number of key negotiations increases. Simulation results and analysis show that 3~4 times repetitious key negotiations are more suitable for high secure connectivity.

【Key words】Wireless Sensor Networks(WSN); key management; secure link; secure connectivity; Cost Performance Ratio(CPR)

随着无线通信、集成电路、嵌入式计算和微机电系统等技术的发展及成熟，传感器网络密钥管理的研究受到广泛关注[1]。本文从理论分析和实验 2 个方面作了分析研究，为新的密钥管理协议的设计和现有密钥管理协议的实现提供了参考。

1 工作模型

1.1 网络模型

本文使用和文献[2]相同的随机网络模型 N 和假设:

$N_r=(V_r, E_r)$

$V_r=\{<x, y>|x=random(area.\ x), y=random(area.\ y)\}$

$E_r=\{<v_1, v_2>|\ distance(v_1, v_2)\leqslant 0, v_1, v_2\in V_r\}$

其中，$random(n)$表示产生一个不大于 n 的随机数；$area.\ x$, $area.\ y$ 表示某一地理区域的长、宽；$distance$ 计算 2 节点间的距离。

本文用 $N_r(A\times B-C)$ 表示在长为 A ft、宽为 B ft 的区域中随机布置 C 个节点形成的随机网络。

1.2 能耗模型

仿真实验能耗测定方法采用 Victor Shnayder 等人提出的 PowerTOSSIM[3]。

1.3 损耗模型

仿真实验的损耗模型采用 Philip Levis 等人提出的位损耗模型和包损耗模型[4]。在损耗模型中包损耗 E_p 和位损耗 E_b 之间存在如下关系[3]:

$$E_p=1-((1-E_b)^9\times((1-E_b)^8+(8E_b\times(1-E_b)^{12}))^d) \quad (1)$$

其中，d 为包长度，单位为 Byte。

2 增加的协商次数

2.1 3 个衡量指标

引入以下 3 个衡量指标，用于衡量在无线传感器网络(Wireless Sensor Networks, WSN)中增加密钥协商次数的有效性。

(1)安全连通率

由文献[2]可知，安全连通率 R_{sl}(Rate of the Secure Links)指经过密钥协商后建立的安全连接数与实际网络连接数(通信范围内所有连接)的比率，它表示密钥协商协议的效率。

$$\forall\ N=(V,E), R_{sl}=L_s(N)/L(N)\times 100\% \quad (2)$$

其中，$N\in\{N_g, N_r\}$；$L_s(N)=\sum_{v_i\in V}L_s(v_i)$；$L(N)=\sum_{v_i\in V}L(v_i)$；$L_s(v_i)$计算给定网络节点安全连接数，其值在密钥协商完成后测得；$L(v_i)$计算给定网络节点连接的总数，其值在具体网络模型确定后测得。

(2)加权安全连通率

由文献[2]可知，加权安全连通率 R_{wsl}(Rate of the Weighting Secure Links)指经过密钥协商后建立的安全连接数加权值与实际网络连接数加权值的比率。

$$\forall\ N=(V,E), R_{wsl}=L_{ws}(N)/L_w(N)\times 100\% \quad (3)$$

其中，$L_{ws}(N)=\sum_{v_i\in V}\min[L_s(v_i), L_w(v_i)]$；$L_w(N)$计算给定网络 N 的加权连接总数；$L_w(N)=\sum_{v_i\in V}L_w(v_i)$；$L_w(v_i)=\sum_{e_{ij}\in E}((1-E_p(e_{ij}))$，$e_{ij}=<v_i, v_j>$；$L_s(v_i)$在实验中测定；$E_p(e_{ij})$通过式(1)，由 E_b 及损耗模型求得。

(3)性价比(Cost Performance Ratio, CPR)

为了更好衡量增加密钥协商次数的有效性，本文定义了

基金项目：怀化学院科研基金资助项目(HHUY2008-04)
作者简介：孙发军(1976－)，男，讲师、硕士，主研方向：无线传感器网络及其安全；周志强，副教授、硕士；张 文，讲师、硕士
收稿日期：2008-12-21 **E-mail：**sfjpaper@163.com

一个新的衡量指标——CPR。

定义 1 增加协商次数的 CPR，是指增加一次密钥协商安全连通的提高率与所需代价增加率的比值，此代价包括因协商次数增加引起的能耗代价和延迟时间的代价(共享主密钥协议中延迟时间越大，安全性越低)。

因此，第 i 次增加的密钥协商的性价比计算如下：

$$CPR_i = \frac{\Delta R_{sl_i} / \Delta R_{sl}}{(\Delta p_i / \Delta p + \Delta t_i / \Delta t)} \tag{4}$$

其中，ΔR_{sl_i} 为第 i 次安全连通率的提高值；ΔR_{sl} 为增加 n 次协商后安全连通率的提高值；n 为增加的最大协商次数；Δp_i 为第 i 次能耗代价增量；Δp 为增加 n 次协商后能耗代价总增量；Δt_i 为第 i 次延迟时间代价增量；Δt 为增加 n 次协商后延迟时间代价总增量。

因为加权安全连通率的区分度显著[2]，所以仿真实验用加权安全连通率的提高值来衡量 CPR。

2.2 有效性分析

(1)协商次数对安全连通率的影响

$\forall\ N=(V,E)$，设 S_i 为某链路第 i 次协商成功建立安全连接的概率，则第 n 次协商成功的概率为

$$P\{X=n\}=\prod_{i=1}^{n-1}(1-S_i)\times S_n$$

因此，某链路在 n 次内密钥协商成功的概率为

$$P\{X\leqslant n\}=S_1+(1-S_1)\cdot S_2+\cdots+\prod_{i=1}^{n-1}(1-S_i)\cdot S_n$$

设每次协商成功的概率 S_i 相等，为均值 $\overline{S}$，则该链路在 n 次内成功建立安全连接的概率为

$$\overline{P}\{X\leqslant n\}=1-(1-\overline{S})^n$$

期望的网络安全连通率为

$$\overline{R}_{sl}=\sum_{e_{ij}\in E}\overline{P}\{X\leqslant n\}/\sum_{e_{ij}\in E}1=\overline{P}\{X\leqslant n\}=1-(1-\overline{S})^n \tag{5}$$

由式(5)可知，当 $1-\overline{S}<1$ 时，随 n 的增大，$\overline{R}_{sl}$ 逐步逼近 1，并在 n 较小时逼近速度较快；当 $1-\overline{S}=1$ 时，$\overline{R}_{sl}=0$。

(2)协商次数对能耗的影响

因为每增加一次密钥协商，会增加一定的 CPU 操作和 Radio 通信，所以每增加一次密钥协商，也会增加一次耗能。设节点初始化平均能耗为 $\overline{p}_{\text{initialize}}$，某次密钥协商平均能耗为 $\overline{p}_{r\_s}$，协商期间监听的平均能耗为 $\overline{p}_{\text{listen}}$，则网络节点在 n 次协商期间的平均耗能估算为

$$\overline{p}_{\text{total}}=\overline{p}_{\text{initialize}}+n\times(\overline{p}_{r\_s}+\overline{p}_{\text{listen}}) \tag{6}$$

可见，节点的能耗随协商次数呈线性增长。

(3)协商次数对延迟时间的影响

设节点平均初始化时间为 $\overline{t}_{\text{initialize}}$，所有节点一次密钥协商平均耗用时间为 $\overline{t}_d$，则所有节点 n 次协商后总耗时间期望为

$$\overline{t}_{\text{total}}=\overline{t}_{\text{initialize}}+n\cdot\overline{t}_d \tag{7}$$

其中，节点 v_i 为完成一次密钥协商所需时间，由式(7)可知延迟时间期望也随协商次数呈线性增长。

综上所述，随着协商次数 n 的增加，密钥协商获得的 CPR 越来越低。

3 仿真实验

3.1 仿真实验环境

本仿真实验在 TinyOS1.1.15 的 TOSSIM 环境下进行。仿真的网络模型是长宽均为 390 ft 的正方形区域中的随机网络，协议为修改的 BROSK 协议[5]。

3.2 仿真协议

(1)无确认协商方式

本文仿真的 BROSK 协议采用无确认协商方式。电源能量是无线传感器网络的重要资源，所有部件中耗能最大的是 Radio 通信[4]。通过减少通信数据量(如密钥协商中协商的信息量和包数)达到节能目的，因此，密钥协商中的确认帧不返回，可降低通信能耗。

密钥管理协议可在网络路由协议之前和网络路由协议之后工作。当在路由协议之前工作时，网络中的每个节点都不知道自己有多少邻居，有哪些邻居。密钥协商在广播发现可信邻居后，告知其节点的安全信息时，邻居可不返回确认帧。由于邻居在广播自己的安全信息时会返回该确认帧，因此当密钥协商在路由发现之前工作时，邻居可不返回确认帧，只需

A—>*: Type$\|ID_A\|N_A$

本文称上述方式为无确认(或称不可靠)协商方式，相应的协议称无确认协商协议。

(2)修改后的无确认 BROSK 协议

Step 1 节点 A 向其邻居广播一个密钥协商包

A—>*: Type$\|ID_A\|N_A$

Step 2 节点 A 的邻居收到数据包后，计算并存储 A 的安全信息。

3.3 多次协商仿真

检验密钥协商次数对安全连通率、延迟时间和能耗的影响，本文在 TOSSIM 中对网络 N_r(390×390–400)进行密钥协商仿真，考察多次协商对不同质量通信链路的影响，以取得最佳协商次数。

(1)协商次数对安全连通率的影响

本文将协商次数对安全连通率的影响进行仿真实验，结果如图 1 所示，可以看出，最初几次协商对安全连通率的影响很大，但在第 4 次后，安全连通率的提高不明显。

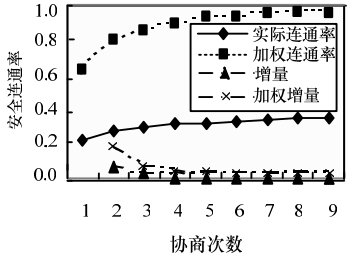

图 1 协商次数对安全连通率的影响

(2)协商次数对不同类型链路加权安全连通率的影响

由图 1 可知，在链路状况较差的 WSN 中，多次协商对安全连通率的提高相对于能耗和延迟时间不可行，但按链路质量分类分析后确定是可行的。

本文将协商次数对不同类型链路加权安全连通率的影响进行仿真实验，结果如图 2 所示。

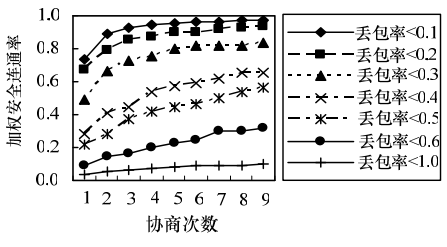

图 2 协商次数对不同类型链路加权安全连通率的影响

由图 2 可知，协商次数的前 3 次增加使丢包率小于 0.3 的链路的加权安全连通率增长很快，其值达到 0.7 以上，且通信质量一般的链路增长也不慢，可见，多次协商有利于通信质量好的链路建立安全连接，协商次数取 3~4 为宜。

(3)协商次数对能耗与延迟时间的影响

为考察增加协商次数对能耗和延迟时间的影响，仿真实验记录多次密钥协商的能耗及安全连接建立后的延迟时间，如图 3、图 4 所示。仿真结果证明随着协商次数的增加，节点的能耗和延迟时间呈线性增长。

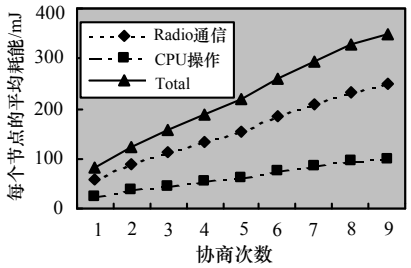

图 3　协商次数对能耗的影响

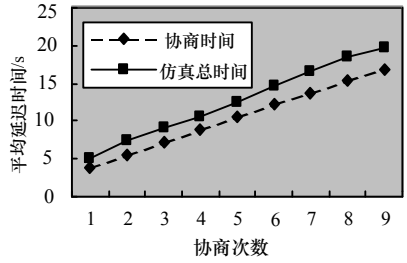

图 4　协商次数对延迟时间的影响

(4)增加协商次数的有效性

根据上文仿真实验的结果，结合式(4)得重复密钥协商的性价比，如图 5 所示。

综上所述，最初增加的几次密钥协商能产生较高的性价比，而到第 3 次后性价比明显降低。

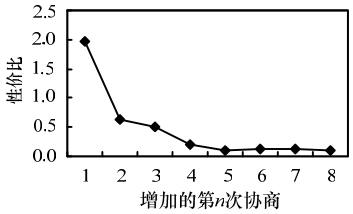

图 5　多次密钥协商取得的性价比

4　结束语

在通信质量不高的 WSN 中进行密钥协商，安全连通率和加权安全连通率都较低，但理论分析和实验证明，通过多次密钥协商后能使加权安全连通率趋近于 1，多数通信质量较高的链路能建立安全连接。提高安全连通率的方法很多，如根据所收到的协商包个数等信息有启发性地进行再次协商也是值得研究的问题，本文今后工作将从该方面展开。

参考文献

[1] Camtepe S A, Yener B. Key Distribution Mechanisms for Wireless Sensor Networks: a Survey[R]. Department of Computer Science, Rensselaer Polytechnic Institute, Tech. Report: 0507, 2005.

[2] 吴　昊, 孙发军, 智云生. 无线传感器网络链路状况对密钥协商的影响[J]. 计算机工程, 2008, 34(10): 138-140.

[3] Shnayder V, Hempstead M, Chen B, et al. Simulating the Power Consumption of Large Scale Sensor Network Applications[C]// Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems. NY, USA: ACM Press, 2004: 188-200.

[4] Levis P, Lee N, Welsh M, et al. TOSSIM: Accurate and Scalable Simulation of Entire Tiny OS Applications[C]//Proceedings of the 1st ACM Conference on Embedded Nerworked Sensor System. Washington, USA: ACM Press, 2003: 126-137.

[5] Cheng Bo, Lai C, Hwang D D, et al. Reducing Radio Energy Consumption of Key Management Protocols for Wireless Sensor Networks[C]//Proceedings of the 2004 International Symposium on Low Power Electronics and Design. NY, USA: ACM Press, 2004: 351-356.

编辑　陆燕菲

（上接第 151 页）

提出的算法在水印尺寸相同时，其他过程的计算量与文献[8]的算法相同。

(3)水印质量好。文献[7]给出水印图像的 *psnr*=44.2, *NCC*=0.982，本文相应值分别为 44.740 3, 0.938 7。文献[8]给出的数据是 *psnr*=43.530 1，本文表 1 前 2 行 *psnr* 的最大值为 44.630 5。虽然数据相差不明显，但文献[7-8]在小波系数的高频带嵌入水印，本文算法只在低频带嵌入水印。文献[2]利用低频带和高频带(LH3)嵌入水印作了对比，在完全相同的条件下，当 *psnr* 为 44.4 dB 时，低频带水印不可见，高频带可见，说明低频系数有较大的感觉容量。综上所述，本文算法嵌入的水印质量较好。

5　结束语

本文提出的算法对水印的灰度值经过加权后直接改变宿主图像小波变换的低频系数。其特点是水印信息容量变化范围大，计算简单，对于要求实时性的场合，如视频水印，有明显优势。

参考文献

[1] 章毓晋. 图像工程(上册)[M]. 北京: 清华大学出版社, 2006: 333-348.

[2] 黄达人, 刘九芬, 黄继武. 小波变换域图像水印嵌入对策和算法[J]. 软件学报, 2002, 13(7): 1290-1297.

[3] 王卫卫, 杨　波, 宋国乡. 基于图像小波变换低频系数的数字水印算法[J]. 信号处理, 2001, 17(6): 554-562.

[4] 余燕忠, 王新伟. 基于信噪比的自适应图像水印算法[J]. 计算机工程, 2003, 29(1): 70-71.

[5] 王向阳, 杨红颖, 邬　俊. 一种基于自适应量化的半脆弱图像水印算法[J]. 小型微型计算机系统, 2006, 27(5): 896-900.

[6] 吕振肃, 应　隽, 李　宏. 基于小波变换的低频数字水印嵌入算法[J]. 兰州大学学报: 自然科学版. 2004, 40(6): 39-42.

[7] Hsieh M, Tseng d, Huang Y. Hiding Digitial Watermarks Using Multiresolution Wavelet Transform[J]. IEEE Transactions on Industrial Electronics, 2001, 48(5): 875-882.

[8] 张　冉, 陈向东. 一种基于小波变换的灰度数字水印嵌入技术[J]. 通信学报, 2004, 25(2): 125-130.

编辑　陆燕菲