第35卷 第21期 计 算 机 工 程 2009年11月
Vol.35 No.21 Computer Engineering November 2009
·安全技术· 文章编号：1000—3428(2009)21—0140—04 文献标识码：A 中图分类号：TP393.08

无线传感器网络中的选择转发攻击检测

江长勇，张建明，王良民
(江苏大学计算机科学与通信工程学院，镇江 212013)

摘 要：针对无线传感器网络中现有检测攻击方法需要节点协同或检测硬件的缺点，对选择转发攻击进行研究，提出一种基于信任度与丢包行为的检测方法。通过节点收发数据包的情况，计算节点的信任度，结合节点丢包行为评估，判断节点是否发动攻击。这种检测方法的计算与存储开销都集中于基站，且不需增加额外的检测设备。实验结果表明，这种方法较之现有检测方法，检测率更高。

关键词：无线传感器网络；选择转发攻击；丢包行为评估；信任度

Selective Forwarding Attack Detection in Wireless Sensor Networks

JIANG Chang-yong, ZHANG Jian-ming, WANG Liang-min
(School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013)

【Abstract】 According to the drawbacks that methods of attack detection in wireless sensor networks require cooperation of nodes or hardware, selective forwarding attack is studied and a light-weight method based on trust degree and behavior of packet loss is proposed. The method detects the attack by calculating trust degree and evaluating behavior of packet loss of nodes, which are based on statistics of receiving and forwarding packets. The calculating and storage pressure of the method are concentrated on the base station and the method works without auxiliary equipment. Experimental results show that the method has relatively higher detection rate than existing methods.

【Key words】 wireless sensor networks; selective forwarding attack; behavior evaluation of packet loss; trust degree

1 概述

在无线传感器网络的选择转发攻击中，恶意节点会拒绝转发并丢弃一些特定的数据包，使得信息不能继续传播。当恶意节点恰好处在数据传输的路径上时，此类攻击的危害最大。目前，国内外针对防范无线传感器网络选择转发攻击的研究很少。文献[1]首先提出利用多路径路由抵御选择攻击。在多路径路由中，信息通过缠绕多路径[2]发送到目的节点，利用多路径的冗余性提高恶意节点控制数据流的难度。但多路径的通信开销会随着路径数目的增加而迅速增加。文献[3]提出了一种基于检查点的多点确认方案来检测选择转发攻击。随机选取路径中的部分节点为检查点，负责包的确认。文献[4]提出利用模糊逻辑抵御选择转发攻击，根据网络能量以及恶意节点数，采用模糊逻辑的方法确定建立的多路径的数量。但这种方法需要用到额外的硬件设备，增加了硬件开销。Watchdog[5]机制同样也可用于选择转发攻击的检测，但需要节点间的协商，节点的能量开销较大。

本文提出了一种基于信任机制与节点行为的选择转发攻击检测方法：根据节点收发数据包的情况计算出节点的信任度，评估节点的行为，找出恶意节点。本文方法的优点是：整个检测机制的计算与存储开销都集中于基站，节点之间无需协商且不需增加额外的硬件设备。

2 假设

本文方法基于如下假设：(1)在部署阶段，传感器网络处于完全安全的状态，攻击者无法俘获网络中的任何节点。(2)节点保持与基站的时间同步(可以采用某些机制加以实现[6])。(3)传感器节点上已采用某种路由协议建立路由(例如INSENS[7]协议)，且基站获取了路由的拓扑，网络已进入数据传输阶段。

此外，本文约定：(1)在数据传输路径上，源节点方向为上游，目的节点方向为下游。(2)在数据传输路径上的2个相邻的节点中，称上游节点 i 与下游节点 i+1 组成一个相邻节点对$(i,i+1)$。

3 基于信任度与丢包行为的入侵检测方法

针对现有检测选择转发攻击的方法需要节点协同或附加硬件的局限性，本文方法仅需根据节点转发数据包的情况，结合信任度计算与丢包行为评估的方法检测攻击。

3.1 检测流程

本文方法设定了一个时钟周期，当源节点向基站发送收集到的数据时，数据传输路径上的节点在时钟周期结束后，统计此时钟周期内，从源节点到目的节点的传输方向上，接收与发送数据包的数量通过报告包(如图 1 所示)，经过密钥加密后发送给基站。

Dst	Src	R_i^t	S_i^t	t_n	$MAC_{K_{<B,i>}}$

图1 报告包

在数据包中，Dst 和 Src 分别是目的节点的 ID 与生成此报告包的节点 i 的 ID；R_i^t 和 S_i^t 分别是节点 i 在时钟周期 t 之内接收与发送数据包的数量；t_n 字段用来指定 R 与 S 所对应的时间段 t；$MAC_{K<B,i>}$的内容为 $MAC_{K<B,i>}\{R_i^t,S_i^t,t_n\}$，是对 R_i^t, S_i^t, t_n，以及这3个字段的摘要。节点 i 部署前就与基站共

基金项目：国家自然科学基金——青年科学基金资助项目(60703115)；江苏省自然科学基金青年科技人才创新基金资助项目(BK2007560)；江苏大学高级专业人才科研启动基金资助项目(05JDG020)
作者简介：江长勇(1983－)，男，硕士研究生，主研方向：传感器网络安全技术；张建明，教授、博士；王良民，讲师、博士
收稿日期：2009-05-08 **E-mail：**onlyjcy@163.com

享密钥 $K<B,i>$，防止恶意节点篡改报告包。

基站设置一个计时器，从时钟周期结束时开始计时。计时器时限为路由中距离基站跳数最大的节点与基站之间进行一次单向数据包传递的时间(可通过初始化时节点与基站的几次交互获得)。超时后，基站根据接收到的报告包，检测路径上 2 个相邻节点之间是否丢包，并计算丢包的数量。为避免检测数据过少给检测结果带来的不利影响，令基站以相邻节点对为单位，每 m 个时钟周期更新一次相邻节点对的信任度，评估丢包行为，做出一次攻击判断。当相邻节点对的信任度小于阈值或被认为行为异常时，基站认定网络存在攻击。

整个检测方法的流程如图 2 所示。

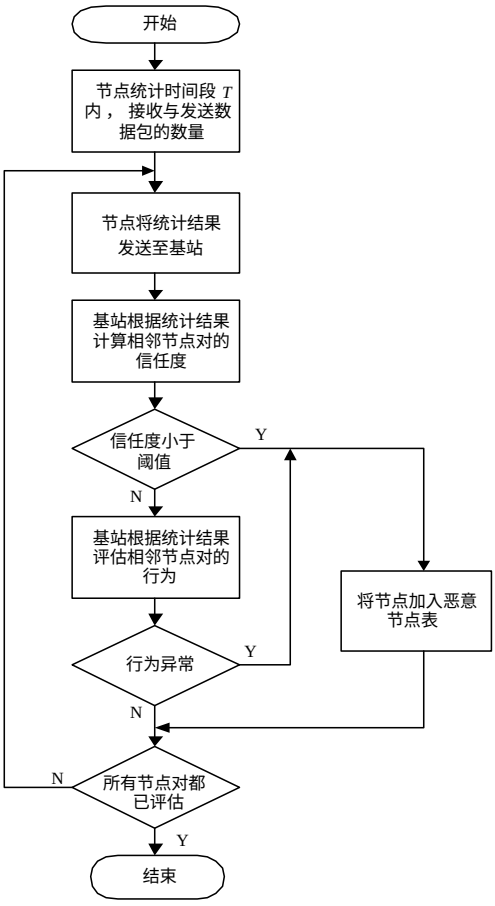

图 2　检测流程

3.2　检测准备

记节点 i 在时钟周期 t 内接收和发送数据包的数量分别为 R_i^t 和 S_i^t。时钟周期 t 结束后，节点将 R_i 和 S_i 发送给基站，如图 3 所示。

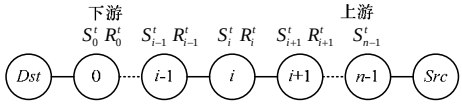

图 3　传输报告包

图 3 中下游到上游的 n 个节点依次编号为 0,1,…,n-1。令 $L_{<i,\ i+1>}^{t}=S_{i+1}^{t}-R_i^t$，用于计算相邻节点对中上游节点发送与下游节点接收数据包数量之差。当 $L_{<i,\ i+1>}^{t}$不为 0 时，节点 i 与 i+1 之间肯定由于某种原因产生了丢包：可能是信道丢包(比如碰撞导致丢包)造成的，也可能是恶意节点丢包造成的。引入主观信任模型，以相邻节点对为实体，以基站为中心建立起一个集中式信任机制。基站对相邻节点对的信任度以一个 0~1 之间的实数 Tr 来表示。Tr=0 表示完全不信任，Tr=1 表示完全信任。本文规定，基站对相邻节点对的信任程度与此相邻节点对的丢包行为对全部丢包行为的影响程度成反相关：对全部丢包的影响越大，相邻节点对的信任度越低；反之，影响越小，信任度越高。采用一个矩阵 $\boldsymbol{A}((n\text{-}1)\times m)$来存放路径上 2 个相邻节点之间，上游节点发送数据包数量与下游节点接收数据包数量之差为 L。统计的时间长度为 T（T 为 m 个时钟周期）。如式(1)所示，$L_{<i,\ i+1>}^{t}$中的 i 和 i+1 为一个相邻节点对，i 的取值范围为 0~n-2，t 为 L 对应的时钟周期，取值范围为 0~m-1。

$$\boldsymbol{A}=\begin{bmatrix} L_{<n-2,n-1>}^{0} & \cdots & L_{<n-2,n-1>}^{j} & \cdots & L_{<n-2,n-1>}^{m-1} \\ & & \cdots & & \\ L_{<i-1,i>}^{0} & \cdots & L_{<i-1,i>}^{j} & \cdots & L_{<i-1,i>}^{m-1} \\ & & \cdots & & \\ L_{<0,1>}^{0} & \cdots & L_{<0,1>}^{j} & \cdots & L_{<0,1>}^{m-1} \end{bmatrix} \tag{1}$$

当 L 不为 0 时，用 $a_{<i,\ i+1>}^{t}$表示相邻两节点对是否发生丢包。$a_{<i,\ i+1>}^{t}$的定义如下：

$$a_{<i,i+1>}^{t}=\begin{cases}1 & L_{<i,i+1>}^{t}\neq 0\\ 0 & L_{<i,i+1>}^{t}=0\end{cases} \tag{2}$$

可将矩阵 $\boldsymbol{A}$ 化为一个稀疏矩阵 $\boldsymbol{B}$，$\boldsymbol{B}$ 的秩 $R(\boldsymbol{B})$是 T 时间段中发生丢包的相邻节点对的数量。

3.3　检测步骤

在对网络的状态作出定量计算的基础上，攻击可分为以下几个步骤：

Step1 计算相邻节点对(i,i+1)在时间 T 内丢包的次数和数量：

$$\sum_{j=0}^{m-1} a_{<i,i+1>}^{j} \tag{3}$$

$$\sum_{j=0}^{m-1} L_{<i,i+1>}^{j} \tag{4}$$

Step2 计算时间 T 内路径上丢包发生的总次数与总数量：

$$Sum_a=\sum_{i=0}^{n-2}\sum_{j=0}^{m-1} a_{<i,i+1>}^{j} \tag{5}$$

$$Sum_L=\sum_{i=0}^{n-2}\sum_{j=0}^{m-1} L_{<i,i+1>}^{j} \tag{6}$$

Step3 计算相邻节点对(i,i+1)在时段 T 内丢失数据包的总数占此时段内丢包总数的比例：

$$Pcta_{<i,i+1>}^{T}=\sum_{j=0}^{m-1} a_{<i,i+1>}^{j}\Big/Sum_a \tag{7}$$

丢包的次数占丢包总次数的比例为

$$PctL_{<i,i+1>}^{T}=\sum_{j=0}^{m-1} L_{<i,i+1>}^{j}\Big/Sum_L \tag{8}$$

Step4 分别对式(7)、式(8)赋予权值 W_1，W_2(W_1+W_2=1)，则对式(7)、式(8)加权求和为

$$W_1 Pcta_{<i,i+1>}^{T}+W_2 PctL_{<i,i+1>}^{T} \tag{9}$$

Step5 结合式(5)、式(6)，计算相邻节点对的信任度的观测值：

$$O_{<i,i+1>}^{T}=1-\left(W_1\frac{\sum_{j=0}^{m-1} a_{<i,i+1>}^{j}}{\sum_{i=0}^{n-2}\sum_{j=0}^{m-1} a_{<i,i+1>}^{j}}+W_2\frac{\sum_{j=0}^{m-1} L_{<i,i+1>}^{j}}{\sum_{i=0}^{n-2}\sum_{j=0}^{m-1} L_{<i,i+1>}^{j}}\right) \tag{10}$$

其中，W_1 和 W_2 分别代表丢包次数与丢包数量对丢包行为影响程度的权值。当网络以收集关键信息为主要任务时，仅一

次丢包就可能丢弃关键信息，因此 W_1 应较大；当网络以收集大量数据为主要任务时，丢包的数量对基站最终收集到的数据影响较大，因此 W_2 应较大。

Step6 通过递归的方式完成信任度的计算与更新，相邻节点对$(i,i+1)$的 T 时间段的信任度为

$$Tr_{<i,i+1>}^{T}=(1-\alpha)O_{<i,i+1>}^{T}+\alpha Tr_{<i,i+1>}^{T-1} \tag{11}$$

其中，$O_{<i^{T},i+1>}$为 T 时间段信任度观测值；$Tr_{<i^{T},i+1>}$为 T-1 时间段的信任度，初值为 0.5；α是遗忘因子。为了使过去的信任度对当前信任度的影响随着时间的推移逐渐变小，α应小于 0.5。当 T 小于阈值时，节点 i 与 i+1 都被认为是恶意节点，加入恶意节点列表。

需要注意的是，并不认为信任度大于阈值的相邻节点对中的节点就一定是正常节点。因为恶意节点可能出现如下类型的攻击行为：(1)类型 a：丢包并不持续，在某个单位时间内丢弃大量的数据包后没有再丢包或仅丢弃少量的包；(2)类型 b：持续丢包，但在单位时间内丢弃的数据包较少，甚至某些单位时间内不丢弃包。针对上述情况，对于信任度大于阈值的相邻节点对，采取以下方法评估丢包行为：

Step1 计算 T时间内发生丢包的所有相邻节点的平均丢包的次数和个数：

$$Avg_{a}^{T}=Sum_{a}/R(\boldsymbol{B}) \tag{12}$$

$$Avg_{L}^{T}=Sum_{L}/R(\boldsymbol{B}) \tag{13}$$

其中，$R(\boldsymbol{B})$是矩阵 $\boldsymbol{B}$ 的秩，即 T 时间段内发生丢包的相邻节点对的数量。

Step2 计算相邻节点对$(i,i+1)$丢包次数与平均丢包次数之差，并用 $Avg_a{}^T$ 归一化：

$$Doa_{<i,i+1>}^{T}=\left(\sum_{j=0}^{m-1}a_{<i,i+1>}^{j}-Avg_{a}^{T}\right)\Big/Avg_{a}^{T} \tag{14}$$

计算相邻节点对$(i,i+1)$丢包数量与平均丢包数量之差，并用 $Avg_L{}^T$ 归一化：

$$DoL_{<i,i+1>}^{T}=\left(\sum_{j=0}^{m-1}L_{<i,i+1>}^{j}-Avg_{L}^{T}\right)\Big/Avg_{L}^{T} \tag{15}$$

Step3 因为式(14)和式(15)分别是相邻节点对$(i,i+1)$的丢包次数与丢包数量相对于平均值的偏离程度，所以，将式(14)与式(15)相乘，当结果小于 0 时，表明相邻节点对$(i,i+1)$存在以下 2 种情况之一：(1)丢包数量多而丢包次数少；(2)丢包数量少而丢包次数多。认为表现出上述 2 类丢包行为的相邻节点对中的节点可能存在攻击 Step6 中类型 a 或类型 b 的攻击行为。将节点 i 与 i+1 加入恶意节点列表。整个检测流程的算法描述如下：

```
/*M：set of Malicious nodes*/
M=Ø
if timer of T does't expire
collect S and R from every node on the path
else
   Calculate   Sum_a and Sum_L;
   /*n: a pair of nodes which are successive
   on the path*/
   /*P: nodes are on the path*/
   for each n∈P
    if n have not been evaluated
       Evaluate(n);
     end if
   end for
Evaluat(n);
Calculate Tr<i^T, i+1>, Doa<i^T, i+1> and DoL<i^T, i+1> for each n;
   if(( (Doa<i^T, i+1>*DoL<i^T, i+1>)<0) && (Tr<i^T, i+1><threshold))
      M=M∪{<i,i+1>};
return   0;
```

3.4 攻击分析

本节主要讨论敌方针对本文方法采取的一些对策。

(1)敌方有可能会丢弃上游节点发来的报告包。但这样做起不到作用：在基站获知路径拓扑的情况下，丢弃报告包将会暴露恶意节点自身。

(2)本文提出的检测方法虽然以相邻节点对作为检测单位，但敌方的丢包行为至多使其上游或下游的一个节点被加入恶意节点列表。

(3)恶意节点可能伪造自身的 S 与上游节点的 R 一致，但恶意节点并不能影响其下游节点，下游节点(如果是正常节点)仍会忠实地向基站汇报自身收发数据包的情况。因此，恶意节点的异常丢包仍会被基站发现。

4 仿真及结果分析

4.1 仿真

如图 4 所示，在 TOSSIM[8]仿真环境下，在 2 000×1 500 m^2 的矩形区域内随机分布 400 个传感器节点进行仿真。基站与事件源分别在区域的两端，源节点与基站之间有 10 个节点，节点之间的数据传输速率为 19.2 Kb/s，事件源共生成 5 000 个数据包，分成 10 次传输，每次传输完成后进行一次攻击检测，一次传输时间为 10 s，每次传送 500 个，2 s 为一个时钟周期，信道丢包率在 0～15%之间，$W_1=W_2=0.5$，$\alpha=0.3$，信任度的阈值取 0.7。

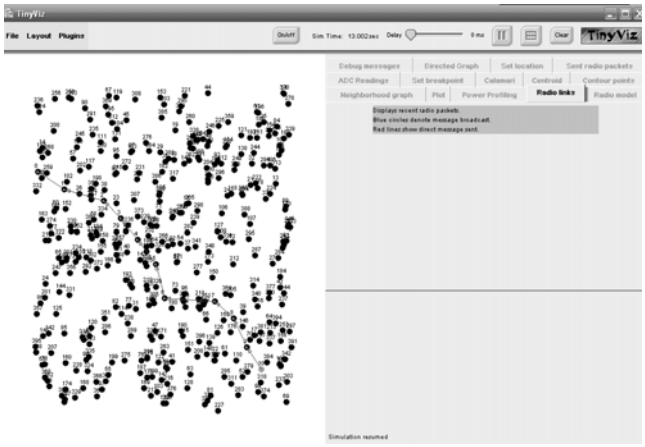

图 4 TOSSIM 中仿真攻击检测

4.2 结果分析

目前检测选择转发攻击的方法主要有：文献[3]采用基于检查点与确认包的方法检测数据传输路径上的异常丢包；文献[5]采用 Watchdog 机制，通过邻居节点间的协商对网络中的丢包进行检测。

由于本文的检测机制与文献[3]的检测机制都是作用于数据传输路径之上的，因此本文将从检测率与误警率 2 个方面与之比较：(1)检测率：检测到的恶意节点的数量与全部恶意节点(包括未检测到的)数量的比值。(2)误报率：非恶意节点数量与全部检测到的恶意节点数量的比值。

在难以判定丢包原因的情况下，信道丢包率增加会导致误警率的增加，但只要恶意节点的丢包行为异常，本文提出的检测机制总能检测到绝大部分存在此行为的恶意节点。

从图 5 可以看出，当路径上的恶意节点数占路径总节点

数的 10%(一个恶意节点)时，本文提出的检测机制的检测率接近 100%；即使在恶意节点占路径上所有节点的 30%时，检测率仍在 95%以上。

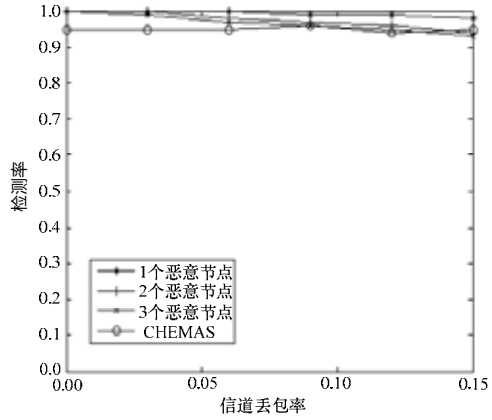

图 5　信道丢包率对检测率的影响

由图 5 和图 6 可以看出，对比文献[3]提出的基于检查点的多点确认方法，本文提出的检测方法在误警率基本持平的情况下能够达到更高的检测率。

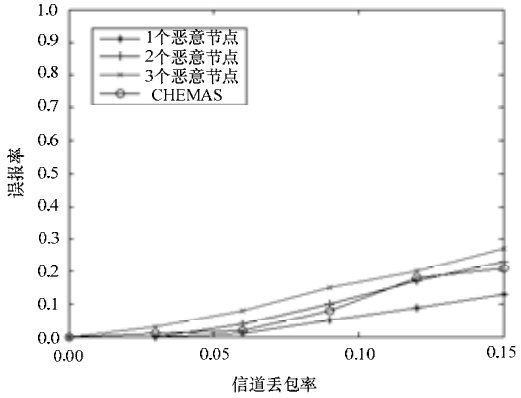

图 6　信道丢包率对误警率的影响

5　结束语

本文从节点行为角度，提出一种基于信任度与丢包行为评估的选择转发攻击检测方法，在避免了额外通信、硬件开销的同时能达到较高的检测率。此外，注意到传输的数据本身也是攻击检测分析的主要对象，因此，如何利用传输的数据进行攻击检测是下一步工作的重点。

参考文献

[1] Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures[J]. IEEE International Workshop on Sensor Network Protocols and Applications, 2003, 1(5): 113-127.

[2] Ganesan D, Govindan R, Shenker S, et al. Highly-resilient, Energy-efficient Multipath Routing in Wireless Sensor Networks[J]. Mobile Computing and Communications Review, 2002, 1(2): 295-298.

[3] Xiao Bin, Yu Bo, Gao Chuanshan. CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks[J]. Journal of Parallel and Distributed Computing, 2007, 67(11): 1218-1230.

[4] Lee H Y, Cho T H. Fuzzy-based Reliable Data Delivery for Countering Selective Forwarding in Sensor Networks[M]. Heidelberg, Germany: Springer, 2007.

[5] Ioannis K, Dimitriou T, Freiling F C. Towards Intrusion Detection in Wireless Sensor Networks[C]//Proc. of the 13th EuropeanWireless Conference. Paris, France: [s. n.], 2007.

[6] Li Qun, Rus D. Global Clock Synchronization in Sensor Networks[J]. IEEE Trans. on Comput., 2006, 55(2): 214-226.

[7] Deng Jing, Han R, Mishra S. INSENS: Intrusion-tolerant Routing for Wireless Sensor Networks[J]. Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, 2006, 29(2): 216-230.

[8] Levis P, Lee N. TOSSIM: A Simulator for TinyOS Networks[EB/OL]. (2003-09-17). http://www.cs.berkeley.edu/~pal/pubs/nido.pdf.

编辑　任吉慧

（上接第 139 页）

签阶段被拒绝。所以，该协议实现了双向认证。同时，如果标签在认证协议的标签应答阶段之后发生掉电，则标签仍然可以通过数据库记录中的 K_p 完成读写器的互相认证，所以该协议很好地解决了标识更新机制中的同步问题。

4　结束语

基于 Hash 锁的同步强化 RFID 安全协议实现了不可追踪性、防止信息泄露和数据同步等安全要求，具有成本低、计算负荷小、健壮性好等优点，基本实现了 RFID 安全隐私保护的需要，是一种较为实用的安全协议。

参考文献

[1] Juels A. RFID Security and Privacy: A Research Survey[J]. IEEE Journal on Selected Areas in Communication, 2006, 24(2): 381-394.

[2] Ohkubo M, Suzuki K, Kinoshita S. Cryptographic Approach to “Privacy-friendly” Tags[C]//Proc. of RFID Privacy Workshop. Cambridge, MA, USA: [s. n.], 2003: 77-83.

[3] Sarma S, Weis S, Engels D. RFID Systems and Security and Privacy Implications[C]//Proc. of Workshop on Cryptographic Hardware and Embedded Systems. [S. l.]: Springer, 2002: 454-469.

[4] Lee S M, Hwang Y J, Lee D H. Efficient Authentication for Low-cost RFID Systems[C]//Proc. of the International Conference on Computational Science and Its Applications. Berlin, Germany: [s. n.], 2005: 6l9-627.

[5] 周永彬, 冯登国. RFID 安全协议的设计与分析[J]. 计算机学报, 2006, 29(4): 581-589.

[6] 李章林, 卢桂章, 辛运帏. 基于 Hash 链的可扩展 RFID 验证协议[J]. 计算机工程, 2008, 34(4): 173-175.

[7] Dimitriou T. A Lightweight RFID Protocol to Protect Against Traceability and Cloning attacks[C]//Proc. of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks. Athens, Greece: [s. n.], 2005: 59-66.

[8] 曾露华, 熊　璋, 张　挺. Key 值更新随机 Hash 锁对 RFID 安全隐私的加强[J]. 计算机工程, 2007, 33(3): 151-153.

编辑　顾逸斐