基于 LEACH 协议的 Sybil 攻击入侵检测机制

陈珊珊[1,2]，杨庚[2]，陈生寿[2]

（1. 南京邮电大学 海外教育学院，江苏 南京 210003；2. 南京邮电大学 计算机学院，江苏 南京 210003）

摘 要：LEACH 协议有效地解决了无线传感器网络（WSN）能耗性问题，但是在安全性方面存在较大的隐患。因此提出了一种改进 LEACH 协议安全性能的 LEACH-S 机制，采用接收信号强度值（RSSI）的 Sybil 攻击入侵检测策略，通过设定合理的阈值启动该机制，即只有在判定可能遭遇 Sybil 攻击时才启动，实验表明该机制能以较少的能耗代价来有效检测出 Sybil 攻击。

关键词：无线传感器网络；Sybil 攻击检测；安全性能；能量消耗

中图分类号：TP393.08 **文献标识码**：B **文章编号**：1000-436X(2011)08-0143-07

LEACH protocol based security mechanism for Sybil attack detection

CHEN Shan-shan[1,2], YANG Geng[2], CHEN Sheng-shou[2]

（1.College of Overseas Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

2.College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China）

Abstract: Low energy adaptive clustering hierarchy (LEACH) could effectively reduce energy consumption of wireless sensor network (WSN). However, a novel security mechanism was proposed based on LEACH protocol called LEACH-S in order to improve the security performance of WSN. The mechanism adopted a received signal strength indicator (RSSI) based policy for Sybil attack detection in WSN, and a reasonable threshold was chosen to initialize Sybil attack detection strategy in which case attack may occur with high possibility. The simulation results show that the mechanism can detect Sybil attack effectively at the cost of low energy consumption.

Key words: wireless sensor network; Sybil attack detection; security performance; energy consumption

1 引言

能耗低的路由协议能较好地适应无线传感器网络（WSN）的特征[1~3]，LEACH 协议[4,5]正是这样一种路由协议，用于减少能耗和提高 WSN 的可扩展性和生命周期[6]。簇头节点管理该簇中的所有节点，并和基站通信来更新各节点的属性，如能量、安全性和容错性等。基站通过簇头节点将命令有效地转发到所有节点。

当前的路由协议受到了很多攻击，如错误的路由转发信息[7]、恶意转发[8]、Sybil 攻击[9]、Sinkhole 攻击[10]、蠕虫病毒[11]和 DDoS 攻击[12,13]等。在基于簇头的网络中，发起 Sybil 攻击的节点由于自身的能量优势往往容易被选为簇头，导致整个簇的信息丢失。因此，Sybil 攻击的检测和抵御变得尤为重要。

本文提出了一个新的基于 LEACH 协议的机制

收稿日期：2010-09-02；**修回日期**：2010-12-20

基金项目：国家重点基础研究发展计划(“973”计划)基金资助项目(2011CB302903)；国家自然科学基金资助项目(60873231)；江苏省高校自然科学基金资助项目(08KJB520006)；江苏省研究生培养创新工程基金资助项目(CX07B_109z)

Foundation Items: The National Basic Research Program of China (973 Program)(2011CB302903); The National Natural Science Foundation of China (60873231); The Natural Science Foundation for Colleges and Universities of Jiangsu Province(08KJB520006); The Innovation Project for Postgraduate Cultivation of Jiangsu Province(CX07B_109z)

LEACH-S，它能帮助 WSN 抵御 Sybil 攻击。这个安全机制只有当网络中很可能发生了Sybil攻击时才启动，所以它可以用低能耗来实现 Sybil 攻击检测。

2 相关研究

Karlof 等人分析了 Sybil 攻击对于 WSN 的危害，提出使用对称加密技术防御 Sybil 攻击[14]。每个节点与一个可信赖的基站共享唯一对称密钥，2 个节点间使用多路质询—回应协议建立共享密钥，相邻节点使用该密钥实现身份验证并加密它们之间的连接。该算法虽然能够较好地节约节点资源，但是因为使用对称密钥安全性能较差，而且基站需要承担较大的工作量，成为网络的潜在瓶颈[15]。

Newsome 等人提出 2 种 Sybil 攻击防御策略[16]：①无线信道检测；② 密钥预分配。无线信道检测的前提是每个物理节点只有一个射频，而且假定每个射频不能同时发送和接收多个信道。当一个节点需要验证其相邻节点是否为 Sybil 节点，它会为每个邻居分配一个信道，并在其上广播信息，然后随机选择一个信道进行监听，如果邻居是合法节点，那么发送节点就会监听到应答消息。但是该策略中的节点如何为邻居节点分配信道问题一直未被解决，且该方法中节点能量消耗过快。密钥预分配方案则随机地从密钥池中选择几个密钥预先存储到各个节点中，传感节点利用这些信息在密钥建立阶段就可以和相邻节点建立共享的密钥，用来保证节点间会话的安全。如果将这些密钥信息和节点的 ID 关联起来，那么攻击者就很难伪造身份 ID，也无法伪造和 ID 相对应的密钥信息，可以有效地抵御 Sybil 攻击。上述这些方案虽然能够在一定程度上抵御 Sybil 攻击，但是对于能量和存储资源非常宝贵的传感器节点来说，能耗代价相对较大[9]。

Murat 等人提出了通过比较同一时刻不同 ID 节点发送消息的接收信号强度值(RSSI, received signal strength indicator)来区别是否发生 Sybil 攻击[17]，但是这种策略会因为无线信道衰耗的不确定性而失效。

本文讨论了 LEACH 协议面临的安全性能问题，针对 WSN 中的 Sybil 攻击，建立了 Jakes 信道模型模拟了无线信道衰减，提出了一种新的基于 RSSI 的 Sybil 攻击入侵检测策略，对簇头数设定适当的阈值，超过该阈值时才启动该入侵检测策略，权衡了整个网络的安全性和能耗性。

3 LEACH 协议的安全性问题

3.1 最优簇头数在 LEACH 协议中的作用

LEACH 协议采用周期性“轮”的概念，每轮包括簇头建立和数据传输 2 个阶段。簇头建立阶段主要负责簇头的产生、分簇管理、TDMA 调度等。数据传输阶段主要负责数据的传输、融合等技术。

在簇头建立阶段，每个节点需要通过概率选择的方法决定是否充当本轮的簇头节点。这主要取决于整个网络中簇头节点占所有节点数目的百分比和这个节点在过去的操作中是否充当过簇头节点。对于一个节点 n，它随机产生一个 0 到 1 之间的数字，称为标志值。如果节点 n 的这个标志值小于一个门限值 $p(r)$，则节点 n 就充当本轮的簇头节点。门限值定义如下：

$$p(r)=\begin{cases}0, & \text{其他}\\ \dfrac{p}{1-p\left[r \bmod \left(\dfrac{1}{p}\right)\right]}, & n\in G\end{cases} \tag{1}$$

其中，$p(r)$为该门限值，r 为当前的轮数。G 为一个集合，该集合中的节点是前 r 轮中从未充当过簇头节点。符号 mod 是求模运算符号。p 表示整个网络中簇头节点占所有节点数目的百分比。

簇头节点的个数与 LEACH 协议的能耗直接相关。如果簇头数过少，簇头节点管理成本会很大，且非簇头节点到簇头节点的传输距离较远，增加了簇头节点及簇内节点的能耗负担；反之，如果簇头数过多，由于簇头节点的大量能耗负担，会导致整个网络的总能耗增大。因此，在建设传感器网络之前，为了减少能耗，需要确定最优簇头数。

根据 LEACH 协议的物理模型[5]，在理想的实验环境中，100 个节点的网络最优簇头数为 $1\leqslant k_{\text{opt}}\leqslant 7$，在真实网络，需要比较 k_{opt} 在不同值间变动时每轮消耗能量的平均值，得出 k_{opt} 的实际最优值。

3.2 Sybil 攻击对 LEACH 协议的威胁

分簇是 LEACH 协议中一个重要的部分，攻击节点一旦成为簇头节点，受影响的不仅仅是该节点周围的邻居节点，而是整个簇域。

Sybil 攻击是一个节点模拟不同节点的 ID 进行恶意行为。如果节点 ID 是由 32bit 整数组成，那么攻击节点通过生成 32bit 随机数就获得多个节点

ID，或者盗用其他合法节点的身份。攻击节点可产生任意多个节点身份 ID，并在一个物理设备上使用。

由于一个 Sybil 节点有几个合法节点身份，就会发送多次广播信号，增加了它被选为簇头节点的概率。而且 Sybil 节点可以通过较大的功率给周围发送广播信号，其他节点会因为该“簇头”节点的 RSSI 值较大而选择加入该簇域，增加了其他节点将其误选为簇头节点的概率，Sybil 攻击节点成为簇头节点并获得了大量节点采集的数据后，就丢弃或者篡改这些数据，使该范围内的网络瘫痪，所有数据都无法到达基站。

4　基于 RSSI 的 Sybil 攻击入侵检测机制

本文提出了一种改进 LEACH 协议安全性能的 LEACH-S 机制。LEACH-S 机制包括引入 Jakes 信道模型[18]，运用基于 RSSI 的 Sybil 攻击入侵检测策略，以及入侵检测启动机制。

节点发送数据的能耗略大于接收数据，两者远大于数据处理和采集的能耗。

无线电传播路径损耗对于 RSSI 的计算有很大影响，仿真环境中常用的传播路径损耗模型有多径衰耗模型[18]、自由空间传播模型[19]、阴影衰落模型[20]等，虽然考虑了无线信号的反射、多径等实际情况，但是在实际应用中还需要综合考虑环境变化等因素对于无线信道的影响。信号的衰减是不可预测的，会受到天气情况等外界因素的影响，而且不同时刻的信道衰落是不一样的。为了提高 RSSI 值计算的精确性，仿真中引入了 Jakes 信道模型。

4.1　基于 RSSI 的 Sybil 攻击检测策略

在 Jakes 信道空间中，接收信号强度是发送端和接收端之间距离的函数，根据接收节点的信号强度可以计算出节点的位置，判断出 WSN 中是否发生 Sybil 攻击。在本文的工作中，考虑如下的网络环境：网络中的所有节点是同构的；网络拓扑结构一旦形成不发生变化。

用 $RSSI_{\mathrm{t}}$ 表示发送信号强度。$RSSI_{\mathrm{t}}=10\lg P_{\mathrm{rec}}$，$P_{\mathrm{rec}}$ 表示节点的接收能量。同一时刻，簇头节点自身的发射能量 $RSSI_{\mathrm{t}}$ 是一定的，信道的冲激响应 H 也认为是相同的，虽然信号的衰减是不确定的，但节点 i 与节点 j 对于簇头节点接收信号强度比是稳定的。

$$\frac{RSSI_i}{RSSI_j}=\frac{RSSI_{\mathrm{t}}\times\|H\|^2\Big/d_i^{\alpha}}{RSSI_{\mathrm{t}}\times\|H\|^2\Big/d_j^{\alpha}}=\left(\frac{d_j}{d_i}\right)^{\alpha} \tag{2}$$

基于 LEACH 协议的 WSN 网络中节点的位置是固定的，节点间的相对位置基本不发生变化，从式(2)可以看出，在同一时刻，簇头发射能量相同的情况下，$RSSI$ 的比值只和距离有关，与 $\frac{1}{d^{\alpha}}$ 成正比，用 $RSSI_i^n$ 表示节点 i 接收另一节点 n 信号时的信号强度，有

$$\frac{RSSI_i^n}{RSSI_j^n}=\left(\frac{d_j^n}{d_i^n}\right)^{\alpha} \tag{3}$$

这里讨论一种检测 Sybil 攻击方法。其中 S_1 和 S_2 是同一个攻击节点的 2 个 ID，D_1、D_2、D_3、D_4 是任意 4 个普通节点作为检测节点，当攻击节点进行网络攻击时，S_1 和 S_2 都会发送广播，4 个节点就能确定节点 S_1 和 S_2 的相对位置。

$$\begin{cases}\dfrac{RSSI_{D_1}^{S_1}}{RSSI_{D_2}^{S_1}}=\dfrac{RSSI_{D_1}^{S_2}}{RSSI_{D_2}^{S_2}}\\[2ex]\dfrac{RSSI_{D_1}^{S_1}}{RSSI_{D_3}^{S_1}}=\dfrac{RSSI_{D_1}^{S_2}}{RSSI_{D_3}^{S_2}}\\[2ex]\dfrac{RSSI_{D_1}^{S_1}}{RSSI_{D_4}^{S_1}}=\dfrac{RSSI_{D_1}^{S_2}}{RSSI_{D_4}^{S_2}}\end{cases} \tag{4}$$

如果式(4)成立，说明 S_1 和 S_2 到 4 个检测节点的距离相等，则 S_1 和 S_2 处于同一位置，所以此时 S_1 和 S_2 为同一个节点，但却是 2 个不同 ID 号，于是检测出发生了 Sybil 攻击。

4.2　入侵检测的启动

传统 LEACH 协议中，普通节点不存储当前网络中选举出的簇头数，只存储每个簇头节点发送广播信息时的接收信号强度值，根据接收信号强度值的大小选择具体加入哪个簇域。在 LEACH 网络中，每次选举的簇头数虽然为一个随机值，但是有一定的规律，一般都在最优簇头数 k 值附近，如果发生了 Sybil 攻击，由于一个 Sybil 簇头有多个 ID，则此时网络中的簇头数会增加，导致很可能簇头数与 k_{opt} 值偏离较大。因此，可以通过检测网络中簇头数的变化，有效地感知是否有 Sybil 攻击产生。

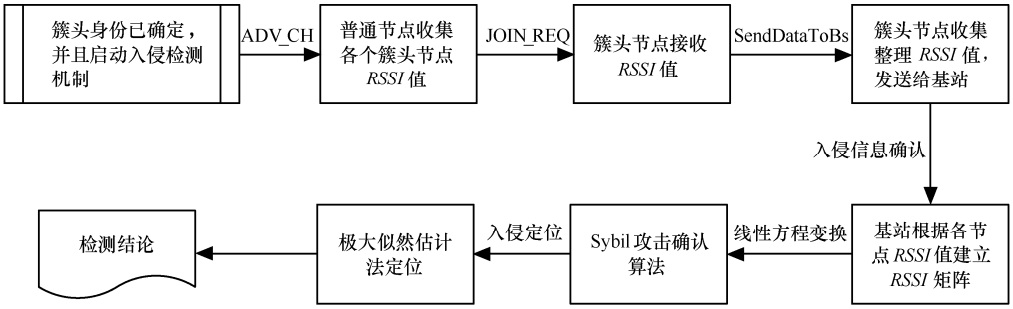


图 1 LEACH-S 机制流程

网络中需要收集当前产生的簇头数，在 LEACH 协议的簇头选举阶段，当簇头节点收到其他簇头节点的广播信息时，都记录该消息，如果检测到当前网络中簇头数目大于一定的阈值时，说明可能发生了 Sybil 攻击，给簇内节点发送 TDMA 时隙表时，捎带当前簇域的簇头节点数，并通知簇内节点当前网络中发生了 Sybil 攻击，让整个网络启动入侵检测策略。

4.3 LEACH-S 机制描述

LEACH 协议中，节点向簇头发送消息时采用 TDMA 调度方式，减少了信道资源的争抢冲突，但是这种机制决定了簇内普通节点间的通信会收到限制，因为在同一时刻，同一簇内只能有一个节点发送数据，其他节点均处于睡眠状态，信道发生冲突时，簇内能量消耗值是正常情况下的好几倍。因此，当检测出网络中可能发生 Sybil 攻击时，LEACH-S 机制则通过簇头节点将相关信息发送给基站，由基站来负责网络攻击事件的确认与定位。具体流程如图 1 所示。

如图 1 所示，当节点发现簇头节点的个数大于预先设定的检测阈值 N_{thread} 时，认为可能发生了 Sybil 攻击，需要启动入侵检测机制，此时，在节点确定其簇头节点后，将收集的各个簇头的 *RSSI* 值发送给簇头节点，簇头节点再负责将此信息发送给基站，在基站收到该信息后，建立 *RSSI* 矩阵，如果通过计算得到了式(4)的情况，证明发生了 Sybil 攻击，通过极大似然估计法就可以定位攻击节点。

5 仿真结果分析

利用 NS2 进行仿真实验，物理参数参考表 1，在 100m×100m 的范围内随机撒播 100 个节点，基站坐标取（50，175）。普通节点的通信半径是 100m，簇头节点的通信半径是 200m。WSN 网络节点分布如图 2 所示。

表 1 LEACH 协议仿真参数

仿真参数	值
电路消耗能量	50 nJ/bit
放大系数（短距离）	0.0013 pJ/bit/m^2
放大系数（长距离）	10 nJ/bit/m^2
数据融合开销	5 nJ/bit/signal
初始能量	2J
每轮之间时间间隔	20s

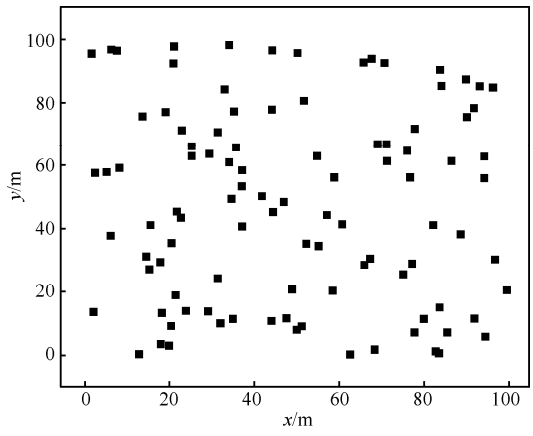


图 2 节点分布

5.1 最优簇头数的确定

簇头节点个数的选择对于 LEACH 协议的运作十分重要，在上述的仿真环境中，实验得出簇头数选择为 4 的时候平均能量消耗最小，因此，将最优簇头数 k 设置为 4，以下其他的仿真结果都基于该值。

5.2 检测机制的启动

跟踪 LEACH 协议网络的簇头选举过程，观察每轮选举的簇头数如图 3 所示，没有发生 Sybil 攻击时，每轮的簇头数相对稳定，一般都在 4 附近。假设 Sybil 攻击节点具备 N 个身份，在选举阶段它将自己伪装为 N 个合法的簇头节点，此时网络内簇

头节点的个数会增加，如果及时捕捉到这种变化，便可以有效地抵御该入侵行为。

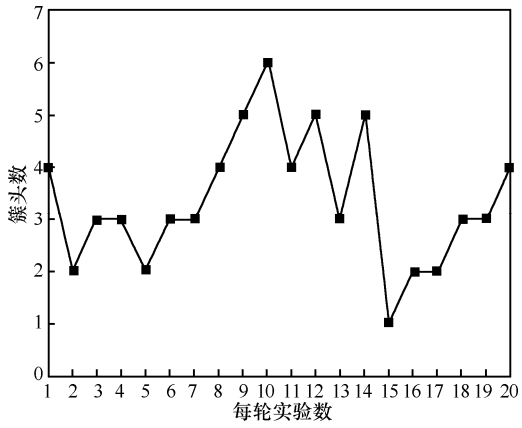


图 3　节点个数

图 4 表明经过多轮实验发现簇头数为 4 的概率最大，大概率事件主要集中于[1,7]之间，如果簇头数大于 7，网络中可能产生了 Sybil 攻击，所以可以在簇头节点数超过 7 时启动相应的入侵检测策略。

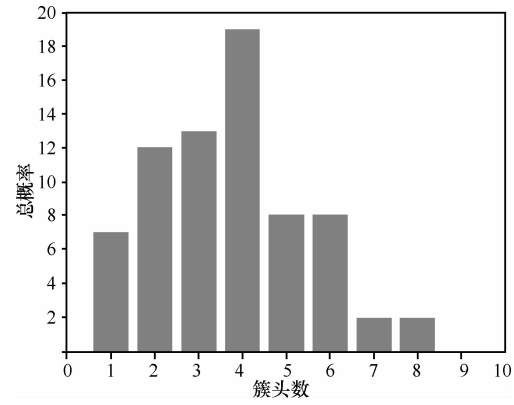


图 4　每轮产生簇头数的概率

5.3　LEACH-S 安全性能分析

用 2 个标准检测率 DR(detection rate)和误报率 FPR(false positive rates)来说明 LEACH-S 机制的安全性能，这部分的仿真是针对所提出的安全机制，对网络中的 2 种安全性能指标进行实验测试和分析。

LEACH-S 是针对 Sybil 攻击的特点设计的安全机制，设定网络内生成簇头数的阈值为 N_{thread}，攻击节点声称自己为簇头节点时，它所具有的 ID 数设为 ID_{thread}，当前产生的簇头数大于 N_{thread} 时，启动 Sybil 攻击入侵检测机制。这里取 ID_{thread} 为 2，N_{thread} 值的选取对于检测结果影响较大，N_{thread} 的取值对安全性能的影响如图 5 所示。

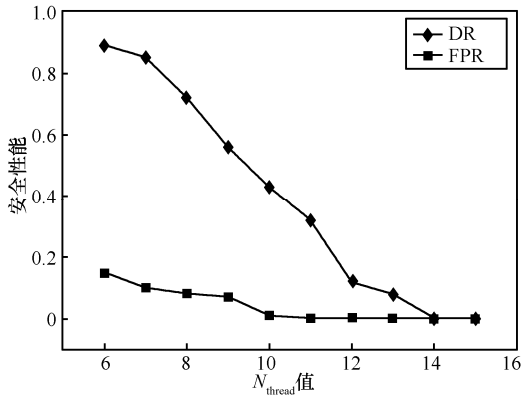


图 5　N_{thread} 对于安全性能的影响

从图 5 可以看出，检测率和误报率随着 N_{thread} 值的增加而降低。因为在 N_{thread} 值较小时，容易触发入侵检测机制，而基站只要能够收集到足够多的 RSSI 信息，便可以定位入侵节点，检测率较高，但是这样会增加误报的概率。检测率无法达到理想状态 1，最高也只有 89%，因为即使簇头数没有达到 N_{thread}，并不表示网络中就一定没有 Sybil 攻击产生，且受到攻击节点的影响，基站并不能保证每次都能够收集到足够多的 RSSI 信息，只有收集到足够多的 RSSI 信息，才能使极大似然估计定位算法的精确度高。综合考虑上述安全性能指标，在后面的仿真中将 N_{thread} 设置为 7。

上面的仿真是 ID_{thread} 取固定值 2 的检测结果，通常在 Sybil 攻击中，ID_{thread} 值是由攻击节点自己决定的，是可变的，讨论不同的 ID_{thread} 值对于安全性能的影响。

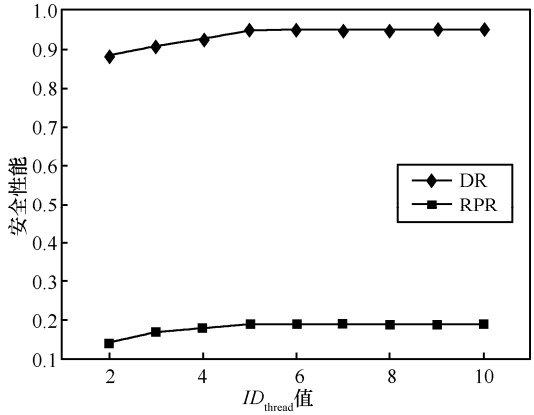


图 6　ID_{thread} 对于安全性能的影响

图 6 中随着 ID_{thread} 的增大，检测率不断增大，误报率也随之增大，而误报率最多只能达到 0.2 左右，所以从入侵检测的角度，ID_{thread} 值越大，该机制越能有效检测出 Sybil 攻击，网络安全性能高。

5.4 LEACH-S 能耗分析

由于节点计算所消耗的能量远小于数据传输的能量消耗，LEACH-S 机制大部分能耗在于数据传输。在网络应用中，假设基站的能量相对于节点来说足够大甚至是有源的，网络节点将现场数据发送给基站，由基站来负责 Sybil 攻击的检测与攻击节点的定位。根据上节讨论，N_{thread} 为 7 时，ID_{thread} 值越大，网络安全性能越高。攻击节点的入侵效果与 ID_{thread} 值的大小成正比，但能量消耗与 ID_{thread} 值也成正比，攻击节点自身对于 ID_{thread} 值的选择会进行权衡，这里将 ID_{thread} 设置为最小值 2。

如图 7 所示，加入了安全机制 LEACH-S 后，网络的生命周期略低于原 LEACH 协议，这是因为在启动入侵检测策略时，LEACH-S 机制中节点需要收集 RSSI 信息并发送给基站，所以需要消耗一些能量，能量消耗比 LEACH 协议略大。仿真过程中还发现，如果每轮实验都启动该入侵检测策略，网络生命周期将减少到一半，实验结果表明在这种情况下安全事务消耗的能量过大。与 LEACH 协议和纯 RSSI 攻击检测策略相比，LEACH-S 安全机制能有效抵御 Sybil 攻击并且能延长网络生命周期。

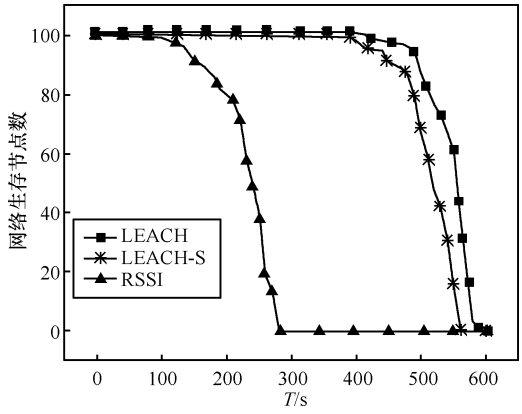


图 7 网络生命周期比较

6 结束语

本文提出了一种改进 LEACH 协议安全性能的 LEACH-S 机制，采用 RSSI 的 Sybil 攻击的入侵检测策略，该入侵检测策略在一定条件下才启动，有效地减少了安全机制对于能量的消耗。Sybil 攻击的特点是会不断更换 ID 来骗取周围节点的信任，每次更换 ID 时，它都会广播消息给邻居节点，并且宣称自己为簇头节点。在 LEACH 协议中，网络中簇头节点的个数不断被收集，正常情况下每轮选举出的簇头的个数相对稳定，而本文的策略是当簇头数超过一定阈值时就启动入侵检测机制。实验表明，该入侵检测启动机制能有效抵御 Sybil 攻击，同时网络的能耗相对较小。在仿真过程引入了 Jakes 信道模型，使 NS2 对于 LEACH 协议物理信道的仿真更加接近于实际情况，仿真数据更加准确。

参考文献：

[1] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, *et al*. Wireless sensor networks: a survey[J]. Computer Networks, 2002, 38(4), 393-422.

[2] SHEU J P, TU S C, YU C H. A distributed query protocol in wireless sensor networks[J]. Wireless Personal Communications, 2007, 41(4): 449-464.

[3] 刘志, 裘正定. 基于分环多跳的无线传感器网分簇路由算法[J]. 通信学报, 2008, 29(3): 104-113.
LIU Z, QIU Z D. Ring based multi-hop clustering routing algorithm for wireless sensor networks[J]. Journal on Communications, 2008, 29(3): 104-113.

[4] HEINZELMAN W R, CHANDRAKASAN A, BALAKRISHNAN H. Energy-efficient communication protocol for wireless micro sensor networks[A]. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences[C]. 2000.

[5] HEINZENLMAN W B, CHANDRAKASAN A P, BALAKRISHNAN H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Transactions on Wireless Communications, 2002, 1(4): 660-670.

[6] JIN Y, WANG L, KIM Y, YANG X. Energy efficient non-uniform clustering division scheme in wireless sensor networks[J]. Wireless Personal Communication, 2008, 45(1): 31-43.

[7] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: attacks and countermeasures[A]. First IEEE International Workshop on Sensor Network Protocols and Applications[C]. Anchorage, AK, 2003. 113-127.

[8] MIZRAK A T, CHENG Y C, MARZULLO K, *et al*. Detecting and isolating malicious routers[J]. IEEE Transactions on Dependable and Secure Computing, 2006, 3(3): 230-244.

[9] MURAT D, YOUNGWHAN S. An RSSI-based scheme for sybil attack detection in wireless sensor networks[A]. World of Wireless, Mobile and Multimedia Networks[C]. Buffalo, New York, USA, 2006. 564-570.

[10] EDITH C H, LIU J C, MICHAEL R L. On the intruder detection for sinkhole attack in wireless sensor networks[A]. IEEE International Conference on Communications[C]. Istanbul, Turkey, 2006, 11-17.

[11] WANG W C, BHARGAVA B. Visualization of wormholes in sensor networks[A]. Proceedings of the ACM Workshop on Wireless Security[C]. Philadelphia, PA, USA, 2004. 51-60.

[12] MIRKOVIC J, REIHER P. A Taxonomy of DDoS attack and DDoS defense mechanisms[J]. ACM SIGCOMM Computer Communication Review, 2004, 34(2): 39-53.

[13] 田俊峰, 朱宏涛, 孙冬冬等. 基于用户信誉值防御 DDoS 攻击的协同模型[J]. 通信学报, 2009, 30(3): 12-20.
TIAN J F, ZHU H T, SUN D D, *et al*. Model of coorperation defense DDoS attack based on client reputation[J]. Journal on Communications, 2009, 30(3): 12-20.

[14] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: attacks and countermeasures[A]. First IEEE International Workshop on Sensor Network Protocols and applications[C]. Anchorage, AK, 2003. 113-127.

[15] ZHANG Q H, WANG P, REEVES D S, *et al*. Defending against sybil attacks in sensor networks[A]. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops[C]. Columbus, OH, USA, 2005. 185-191.

[16] NEWSOME J, SHI E, SONG D, *et al*. The sybil attack in sensor networks analysis & defenses[A]. The Third International Symposium on Information Processing in Sensor Networks[C]. Berkeley, California, USA, 2004. 259-268.

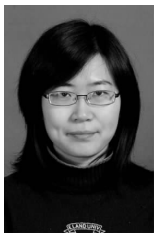
[17] MURAT D, YOUNGWHAN S. An RSSI-based scheme for sybil attack detection in wireless sensor networks[A]. IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks[C]. Niagara-Falls, Buffalo-NY, 2006. 564-570.

[18] LI Y X, HANG X J. The simulation of independent rayleigh faders[J]. IEEE Transactions on Communications, 2002, 50(9): 1503-1514.

[19] WILSON S G, BRANDT-PEARCE M, CAO Q, *et al*. Free-space optical MIMO transmission with Q-ary PPM[J]. IEEE Transactions on Communications, 2005, 53(8): 1402-1412.

[20] BETTSTETTER C, HARTMANN C. Connectivity of wireless multihop networks in a shadow fading environment[J]. Wireless Networks, 2005, 11(5): 571-579.

作者简介：



陈珊珊（1980-），女，安徽安庆人，南京邮电大学讲师，主要研究方向为计算机网络与安全。

杨庚（1961-），男，江苏建湖人，南京邮电大学教授、博士生导师，主要研究方向为网络与移动计算、并行与分布计算。

陈生寿（1984-），男，青海西宁人，南京邮电大学硕士生，主要研究方向为信息安全。