ZigBee 网络抵御 Sybil 攻击的自适应链路指纹认证方案

郁 滨[①] 黄美根*[①] 黄一才[①] 孔志印[②]
[①](解放军信息工程大学 郑州 450004)
[②](信息保障技术重点实验室 北京 100072)

摘 要：该文针对 ZigBee 网络中 Sybil 攻击破坏节点身份唯一性的问题，提出一种抵御 Sybil 攻击的自适应链路指纹认证方案。方案首先基于无线链路特征设计了链路指纹，在此基础上，提出了反映信道质量的相干时间估测算法和适应子节点数量变化的保护时隙(GTS)动态申请算法，并给出了 Sybil 攻击认证流程。安全性分析及实验结果表明，方案在通信环境的安全边界条件下节点认证成功率可达 97%以上，且链路指纹无需存储，具有较低的资源需求。

关键词：无线网络安全；ZigBee；Sybil 攻击；链路指纹；保护时隙
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2016)10-2627-06
DOI: 10.11999/JEIT151476

Adaptive Link Fingerprint Authentication Scheme Against Sybil Attack in ZigBee Network

YU Bin[①] HUANG Meigen[①] HUANG Yicai[①] KONG Zhiyin[②]
[①](*PLA Information Engineering University*, *Zhengzhou* 450004, *China*)
[②](*Key Laboratory of Information Assurance Technology*, *Beijing* 100072, *China*)

Abstract: To solve the problem that Sybil attack damages the uniqueness of node identity in ZigBee network, an adaptive link fingerprint authentication scheme against Sybil attack is proposed. First, a link fingerprint based on the characteristics of wireless link is designed. Based on this fingerprint, two algorithms are presented. One is the estimation algorithm of coherence time reflecting channel's quality and the other is the dynamic application algorithm of Guaranteed Time Slot (GTS) adapting to changes in child node's number. At the same time, the authenticating procedure for Sybil attack is presented. Security analysis and experiment results show that the node authentication rate of the proposed scheme can reach more than 97% under the condition of security boundary in communication environment. Due to the usage of link fingerprint, the scheme has lower resource requirements.

Key words: Wireless network security; ZigBee; Sybil attack; Link fingerprint; Guaranteed Time Slot (GTS)

1 引言

在 ZigBee 网络[1,2]中，Sybil 攻击是一种易于实行而又难于防范的身份攻击方式，核心特征为一个恶意节点设备对外呈现多个 Sybil 节点身份[3]，破坏网络节点身份的唯一性，进而导致基于 ID 标识[4]、身份证书[5]、密钥[6]等依赖于节点存储性能的身份认证措施基本失效[7,8]，网络安全遭受严重威胁。

近年来学者研究发现，以多径效应为核心的无线链路特征可作为通信双方的节点身份标识[9–11]，因其与节点地理位置和通信环境密切相关而难于伪造和窃取[12,13]，逐渐成为防范 Sybil 攻击的新方式。

文献[14]指出在扩频通信方式下，码片内多径可以被分离，近似等价于求解线性方程组，文献[15]进一步将其应用于无线传感器网络基于接收信号强度的定位算法中，在损失一定信噪比的代价下分离出直达径，提高了定位精度。文献[9]基于无线链路多径效应设计了瞬态链路签名机制，通过将新测算的签名样本与安全状态下存储的签名样本比较来区分网络中虚假节点和认证节点，但文献[10]指出其无法抵御模仿攻击，因而引入时间因子，提出时间同步链路签名认证方案，其要求节点时间精确同步，且假设节点物理安全，在价格低廉的 ZigBee 网络中，上述要求与假设不具有现实可行性[16,17]。

文献[11]采用假设检验的方式比对多个节点的信道频率响应是否高度相关来识别 Sybil 节点，方案在静态环境下通过调整相关系数阈值可使 Sybil 节点误检率和漏检率均低于 1%。但是，当通信环境为

收稿日期：2015-12-29；改回日期：2016-05-19；网络出版：2016-07-15
*通信作者：黄美根 huang_meigen@163.com
基金项目：信息保障技术重点实验室开放基金(KJ-15-104)
Foundation Item: Key Laboratory of Information Assurance Technology Open Fund (KJ-15-104)

快衰落信道时，同一链路不同时间的无线链路特征相关度锐减，Sybil 节点漏检率显著增大，且随着节点数量的增多，节点之间的信道频率响应比对次数呈指数增长，最终导致节点资源“供不应求”，从而使方案对通信环境和节点数量的变化不具有自适应性。

综上所述，上述方案存在可行性不高、节点需存储大量链路指纹、通信环境和节点数量适应性欠佳等问题。因此，本文首先通过设计基于多径效应的无线链路指纹，同时提出信道相干时间估测算法和保护时隙(Guaranteed Time Slot, GTS)动态申请算法，实时跟踪通信环境和节点数量变化，最后构造 Sybil 攻击链路指纹认证方案，在估测出的信道相干时间内动态申请通信时隙，采用“零存储”方式对节点组进行链路指纹实时测算与比对，保证网络中节点身份的唯一性，在提高节点认证识别率的同时降低节点资源需求。

2 模型建立

本节首先给出本文的网络结构模型，然后基于多径效应设计了链路指纹，最后在此基础上提出信道相干时间估测算法和 GTS 动态申请算法。

2.1 网络结构

父子关系是 ZigBee 节点之间的一种基本关系，据此对网络分层，最高父节点为协调器，最低子节点为终端，通常假设协调器物理安全，图 1 为抽取网络一层建立的网络结构模型。

定义 1 记 F 表示父节点，$C_p(1 \le p \le m,\ p \in N^*)$ 表示子节点集，其中 m 为子节点数量，$C_{p'}(1 \le p' \le n,\ p' \in N^*)$ 表示合法子节点集，$C_{p''}(n+1 \le p'' \le m, p'' \in N^*)$ 表示被攻击者完全掌控的恶意子节点集，S 表示申请入网的 Sybil 节点，不失一般性，设其附加在恶意节点 C_m 之上。

2.2 链路指纹

在多径通信环境中，接收信号是发送信号多个样本的线性组合，每个样本传播路径不同，传播衰落也不同，且与收发双方的通信链路密切相关。

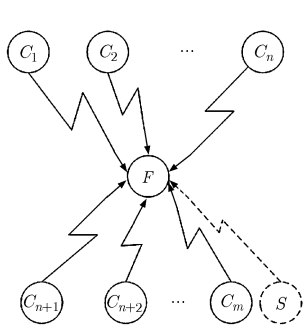

图 1 网络结构模型

定义 2 接收信号中所有多径样本的幅值组成的降序数值序列称为多径幅值序列，记为 $\alpha = \{\alpha_1, \alpha_2, \cdots, \alpha_L\}$，反映了多径环境下的信道冲激响应，通常称首项 α_1 为主径。其中，L 为多径数目，$\alpha_l(1 \le l \le L, l \in N^*)$ 为第 l 条多径信号的幅值。

定义 3 多径幅值序列中所有多径信号幅值与主径信号幅值之比形成的数值序列称为链路指纹，记为 H，如式(1)所示。

$$H = \left\{1, \frac{\alpha_2}{\alpha_1}, \frac{\alpha_3}{\alpha_1}, \cdots, \frac{\alpha_L}{\alpha_1}\right\} \tag{1}$$

定义 4 视 H 和 H' 为 $\hat{L}$ 维空间中的坐标点，则两个坐标点之间的空间距离称为链路指纹距离，记为 δ，计算公式如式(2)所示。

$$\delta = \sqrt{\left(\frac{\alpha_2}{\alpha_1} - \frac{\alpha_2'}{\alpha_1'}\right)^2 + \left(\frac{\alpha_3}{\alpha_1} - \frac{\alpha_3'}{\alpha_1'}\right)^2 + \cdots + \left(\frac{\alpha_{\hat{L}}}{\alpha_1} - \frac{\alpha_{\hat{L}}'}{\alpha_1'}\right)^2} \tag{2}$$

其中 $\hat{L} = \min(L, L')$。

定义 5 设链路指纹距离集合 $\Delta = \{\delta_1, \delta_2, \cdots, \delta_q\}$，则集合各元素的平均值称为链路指纹距离均值，记为 $\overline{\delta}$，计算公式如式(3)所示。

$$\overline{\delta} = \frac{1}{q}\sum_{w=1}^{q}\delta_w \tag{3}$$

其中，$q \in N^*$，$w \in N^*$，$w \le q$。

定义 6 集合 Δ 中明显小于 $\overline{\delta}$ 的元素称为异常距离，其对应的链路指纹 H 与 H' 相同，即对同一接收节点 j，若发送节点 i 和 i' 身份不同则为 Sybil 节点或恶意节点，计算公式如式(4)所示。

$$\delta_w \le \sigma\overline{\delta} \tag{4}$$

其中，$\sigma(0 < \sigma < 1)$ 为链路指纹距离比例阈值。

2.3 信道相干时间

定义 7 信道冲激响应维持高度相关的最大时间间隔称为信道相干时间，记为 T_d，描述了信道对无线信号的衰落节奏。

为使方案能自适应通信环境即信道衰落节奏，设计信道相干时间估测算法如表 1 所示，其中训练序列持续时间记为 T_s，符号 $\lceil\bullet\rceil$ 表示向上取整。算法中，k 为递增变量，由于初始距离集合 Δ 有元素 δ_{12} 和 δ_{13}，因此为保证集合 Δ 的完备性和互异性，k 的初始值为 4。通常，算法估测结果 $T_d \ge 2T_s$。

2.4 超帧 GTS

定义 8 用于限定和分配信道访问时间的特殊帧称为超帧，其活动部分中基础通信时间单元称为时隙片，单个或多个连续时隙片构成的时间段称为保护时隙(GTS)，由协调器负责分配与管理，特定设备使用已分配的 GTS 时无须与其他设备竞争，超帧结构如图 2 所示。

表 1 信道相干时间估测算法

输入：	信道相干时间估测精度 t_ε，最大信道相干时间 T_m，子节点数量 m，训练序列持续时间 T_s，距离比例阈值 σ，$k=4$
输出：	信道相干时间估测值 T_d
步骤 1	父节点 F 广播节点申请入网命令 $\mathrm{Cmd}_{\mathrm{mea}}=\{t_\varepsilon,r\}$，其中 $r=\lceil mT_s/t_\varepsilon\rceil$；
步骤 2	F 间隔时间 t_ε 发送一次训练序列，共发送 $r+1$ 次；
步骤 3	子节点 C_p 依次测算链路指纹，构造指纹序列 $Y=\{H_1,H_2,\cdots,H_{r+1}\}$，计算链路指纹 H_1 和 H_2 的距离 δ_{12}，H_1 和 H_3 的距离 δ_{13}，构造初始距离集合 $\Delta=\{\delta_{12},\delta_{13}\}$；
步骤 4	若 $k=r+2$ 时，跳转步骤 5，否则计算 δ_{1k}，将其加入集合 Δ，判断是否存在不同链路指纹，若存在则跳转步骤 5，否则令 $k=k+1$，跳转步骤 4；
步骤 5	C_p 记 $k^p=k$ 并发送至 F；
步骤 6	F 构造集合 $Z=\{k^1,k^2,\cdots,k^p,\cdots,k^m\}$，记 Z 中出现频次最高(多项相同时取值小者)的项为 k'，记 $T_\varepsilon=(k'-2)t_\varepsilon$，则 $T_d=\min\{T_m,T_\varepsilon\}$。

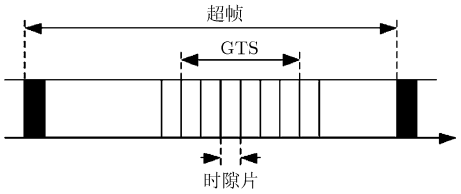

图 2 超帧结构

定义 9　三元组 $\langle M,N,T_s\rangle$ 称为超帧 GTS 申请参数，记为 Γ，计算公式如式(5)和式(6)所示。

$$M=\left\lceil\frac{mT_s}{T_d-T_s}\right\rceil \tag{5}$$

$$N=\left\lfloor\frac{T_d}{T_s}\right\rfloor \tag{6}$$

其中，M 为节点分组数即 F 需申请使用的连续超帧数目，N 为组内最大节点数即一个 GTS 内连续占用的时隙片数目，符号 $\lfloor\bullet\rfloor$ 表示向下取整。

由于协调器资源有限，GTS 申请可能失败，为使方案在 GTS 申请时能自适应节点数量变化，增大申请成功概率，设计 GTS 动态申请算法如表 2 所示。

表 2　GTS 动态申请算法

输入：	子节点数量 m，训练序列持续时间 T_s，信道相干时间估测值 T_d
输出：	GTS 申请结果
步骤 1	依据式(5)和式(6)计算 M 和 N，构造 Γ；
步骤 2	F 发送 GTS 申请命令 $\mathrm{Cmd}_{\mathrm{GTS}}=\{\Gamma\}$ 至协调器申请 GTS，若申请失败跳转步骤 3，否则跳转步骤 5；
步骤 3	令 $N=N-1$，若 $N=1$ 跳转步骤 4；否则由节点分组关系重新计算 $M=\lceil m/(N-1)\rceil$，并构造 Γ，跳转步骤 2；
步骤 4	GTS 申请失败，算法终止；
步骤 5	GTS 申请成功，算法终止。

为在信道相干时间 T_d 内比对链路指纹，申请成功的所有 GTS 中首个时隙片均由申请入网的节点 S 占用并发送训练序列 X。

3　方案流程设计

Sybil 攻击链路指纹认证(以下简称 Sybil 攻击认证)流程启动条件为新节点申请加入网络，方案在估测出 T_d 后，进行 GTS 动态申请，若申请成功，F 将 GTS 以时隙片为单位分配给子节点，用于发送训练序列，使同组节点在 T_d 内全部发送完成，F 则接收训练序列并测算链路指纹，然后比对是否存在相同链路指纹来识别 Sybil 节点，图 3 为 Sybil 攻击认证方案流程。

Sybil 攻击认证方案流程；

步骤 1　节点 S 申请加入网络；

步骤 2　F 执行信道相干时间估测算法，输出信道相干时间 T_d；

步骤 3　F 执行 GTS 动态申请算法，若申请成功跳转步骤 4，否则跳转步骤 10；

步骤 4　F 随机将所有子节点分成 M 组，每组内子节点数为 $N-1$(组内首节点为 S)，最后一组子节点数为 $m-(M-1)\times(N-1)$，分组情况记为 $G=\{G_1,G_2,\cdots,G_M\}$；

步骤 5　F 广播 Sybil 攻击认证命令 $\mathrm{Cmd}_{\mathrm{aut}}=\{\Gamma;G\}$；

步骤 6　所有子节点均依分组情况及超帧参数跟踪超帧，并占用指定 GTS 中时隙片发送训练序列；

步骤 7　F 接收所有训练序列，测算并记录链路指纹，当一个分组处理完毕后，计算该组链路指纹距离，比对判断组内是否存在与 S 相同的链路指纹。若存在，记该节点为 S'，跳转步骤 8，否则继续进行下一分组，当所有分组处理完毕后跳转步骤 9；

步骤 8　S 未通过 Sybil 攻击认证，F 广播拒绝 S 入网命令 $\mathrm{Cmd}_{\mathrm{rej}}=\{S,S'\}$，剔除已入网的节点 S'，跳转步骤 11；

步骤 9　S 成功通过 Sybil 攻击认证，F 广播允许 S 入网命令 $\mathrm{Cmd}_{\mathrm{pas}}=\{S\}$，跳转步骤 11；

步骤 10　GTS 申请失败，F 广播 GTS 申请失败命令 $\mathrm{Cmd}_{\mathrm{los}}=\{S\}$，拒绝 S 入网，Sybil 攻击认证完成；

步骤 11　F 向协调器申请释放 GTS, Sybil 攻击认证完成。

流程中，当连续多个节点申请加入网络时，信道相干时间估测过程可只执行一次，减少频谱占用和资源消耗。

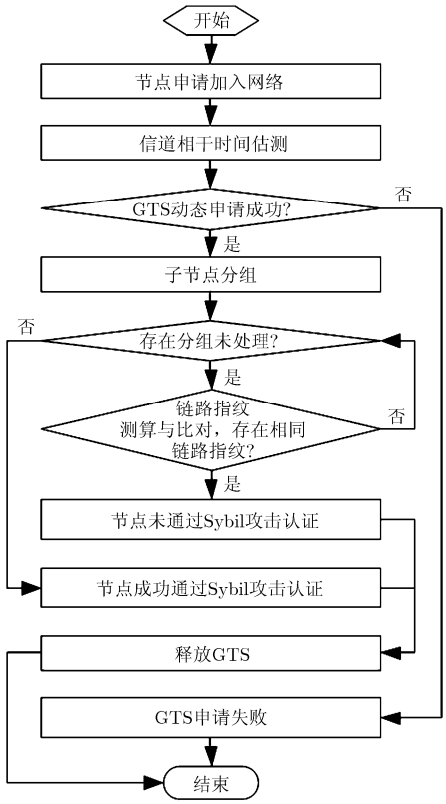

图 3 Sybil 攻击认证方案流程

4 安全性分析

引理 1 两个天线在相距半个波长以上距离时衰落互不相干[12]。

证明 略。

引理 1 为恶意节点对抗无线链路防御手段创造了移动攻击的新方式，即恶意节点使用 Sybil 节点身份时可先移动自身位置半个波长以上再发送数据，造成两者无线链路特征不相关，从而避免被发现；同时，也为无线链路防御 Sybil 攻击指明了方向，即在信道相干时间内，半个波长范围内两个天线的多次同频通信经历的衰落必将高度相关。

定理 1 记 v_m 为恶意节点最大移动速度，λ 为波长，若最大信道相干时间 $T_m \le \lambda/2v_m$，则本文认证方案可有效抵御 Sybil 攻击。

证明 S 加入网络的前提是成功通过 Sybil 攻击认证，对 F 而言，S 应与 C_p 的链路指纹均不相同，即 S 应伪造链路指纹使其与 C_m 不同。因此，攻击者可通过捕获攻击、篡改攻击和移动攻击等方式伪造链路指纹，以此欺骗父节点，从而通过 Sybil 攻击认证。下面对上述 3 种攻击分别进行论证。

(1)捕获攻击：通信环境中无线链路特征实时变化，过期的链路指纹无法有效表征节点身份。在本文方案中，链路指纹实时测量、实时计算、实时比对，且均不进行存储，即链路指纹具备“零存储”特征。同时，方案未采用依赖节点存储密钥安全的加密机制。因此，攻击者无法从被捕获的节点中获取任何与链路指纹相关的信息，方案可有效抵御捕获攻击。

(2)篡改攻击：本文方案链路指纹利用多径效应中各多径样本幅值比值形式设计，与具体各多径样本幅值量值无关，因此攻击者通过篡改节点无线信号发送功率等方式失效。同时，方案中均由接收节点实时测算与发送节点间的链路指纹，即由父节点测算待认证子节点的链路指纹，因此，方案可有效抵御篡改攻击。

(3)移动攻击：由引理 1 可知，攻击者若想成功发动移动攻击，则节点 C_m 必须在时间 T_d 内至少移动距离 $\lambda/2$ 后以 S 的身份发送训练序列，即 $v_m T_d > \lambda/2$。因此从防御角度分析，方案信道相干时间估测值应满足 $T_d \le \lambda/2v_m$，结合信道相干时间估测算法中 $T_d = \min\{T_m, T_\varepsilon\}$，当 $T_m \le \lambda/2v_m$ 时方案可有效抵御移动攻击，也即安全边界条件为 $T_m \le \lambda/2v_m$。

基于上述分析，在安全边界条件内，攻击者无法通过发送捕获攻击、篡改攻击或移动攻击等方式伪造链路指纹，因而无法通过 Sybil 攻击认证。因此，本文方案可有效抵御 Sybil 攻击。 证毕

表 3 是本文方案与文献[10]，文献[11]的方案在安全性能方面的对比。文献[10]是引入时间因子的瞬态链路签名身份认证方案，文献[11]是基于信道频率响应的 Sybil 攻击检测方案，两者分别是基于无线链路特征对 Sybil 攻击进行认证和检测的重要文献，与其进行安全性比较具有普遍意义。结合定理 1，由表 3 可知，本文方案相比文献[10]和文献[11]方案，能够同时抵御捕获攻击、篡改攻击和移动攻击，具有更高的安全性能。

表 3 方案安全性对比

方案	捕获攻击	篡改攻击	移动攻击
本文方案	√	√	√
文献[10]方案	×	√	√
文献[11]方案	√	√	×

5 实验及结果分析

ZigBee 节点采用 CC2530 芯片，通过修改节点固件程序，使其在接收信号的同时完成链路指纹测算，并上传上位机。ZigBee 网络通信信道设为 25 号信道，中心频率为 2475 MHz，最大数据传输速率

为 250 kb/s，采用直接序列扩频和偏移正交相移键控调制技术，基带码元为半正弦脉冲形式，码片长为 32 位，码元宽度为 1 μs，训练序列采用保留参数下的最短物理层帧。

5.1 实验方案

为验证方案安全性能与自适应性能，实验申请入网节点共设计 50 个，其中 25 个 Sybil 节点，25 个合法节点，入网顺序随机。同时，实验环境设定两种，分别为办公场所和公路转盘，前者与文献[11]中实验环境基本一致，属于典型室内多径环境，后者为通信环境实时变化的室外多径环境。方案参数设置如表 4 所示。

表 4 参数设置

参数	含义	取值
m	子节点数量	80
n	合法子节点数量	55
t_ε	信道相干时间估测精度	192 μs
T_s	节点训练序列持续时间	384 μs
σ	链路指纹距离比例阈值	0.25
v_m	恶意节点最大移动速度	60 km/h

在直接序列扩频通信中，接收器数字基带模块中解调信号时需生成与接收信号相位相同的本地伪随机码，并利用伪随机码的自相关峰值特性完成相位对齐，最后在所有的路径分量中选择峰值最强的路径分量用于解调信号[18]。在此基础上，本文方案收集所有路径分量峰值，作为链路指纹测算的多径信号幅值输入。

5.2 实验结果

在上述实验方案的基础上，针对两种环境分别独立实验 1000 次，记录节点的 Sybil 攻击认证情况、信道相干时间估测值、GTS 动态申请占用数等。

(1)安全性结果：汇总 Sybil 节点认证情况，在办公场所实验环境下，Sybil 攻击认证中合法节点识别错误率为 0.81%，即共有 203 个合法节点未通过 Sybil 攻击认证，Sybil 节点识别错误率为 0.86%，即共有 214 个 Sybil 节点成功通过了 Sybil 攻击认证，实验结果略优于文献[11]，且其适应场景是本文的一种情况；在公路转盘实验环境下，合法节点识别错误率为 1.18%，即共有 295 个合法节点未通过认证，Sybil 节点识别错误率为 2.23%，即共有 572 个 Sybil 节点成功通过了认证，相比于静态室内环境而言，节点识别错误率均略有提升，但仍在可接受范围内。

(2)自适应性结果：汇总相关实验数据，在办公场所与公路转盘实验环境下的信道相干时间平均估测值分别为 5037.3 μs 和 1394.6 μs，公路转盘环境下恶意节点处于移动状态，信道衰减快，信道相干时间估测算法的输出值明显小于前者，表明方案对通信环境具有自适应性；在此基础上，GTS 动态申请平均占用数分别为 16.8 个和 42.3 个，节点分组数即 GTS 动态申请算法的输出值也明显大于前者，表明方案对节点数量同样具有自适应性。

5.3 性能分析

分别对本文方案进行存储开销、通信开销和计算开销的分析，网络节点采用短地址标识。

(1)存储开销：假设网络中所有节点均以白名单方式存储合法节点，则子节点仅需存储合法节点白名单，所需存储空间为 $2m$ B；父节点还需存储表 4 中的参数及取值，因此父节点所需存储空间为 $2m+4$ B。

(2)通信开销：通信开销用节点需发送额外报文数量表示。Sybil 攻击认证流程中，父节点需广播 $\lceil mT_s/t_\varepsilon \rceil + 6$ 次报文，子节点需发送 2 次估测值，父节点以广播形式发送报文有效减少了通信开销。

(3)计算开销：计算开销集中在链路指纹测算与比对过程。由方案可知，链路指纹测算采用路径分量峰值，没有增加额外计算量；比对过程中，父节点需多次计算链路指纹距离，计算开销为 $o(n)$，相应子节点计算开销为 $o(1)$。

与安全性对比相对应，本文仍选择与文献[10]，文献[11]进行开销对比分析，如表 5 所示。由表 5 可知，本文方案子节点开销明显优于其他方案，父节点存储开销较小，通信开销略少于文献[10]，计算开销略多于文献[11]，同时本文方案提供了对通信环境和节点数量更强的自适应性，节点识别成功率在快衰落环境中有较大提升，安全性较高。

表 5 方案开销对比

方案	存储开销(B)	通信开销	计算开销
本文父节点	$2m+4$	$\lceil mT_s/t_\varepsilon \rceil + 6$	$o(n)$
本文子节点	$2m$	2	$o(1)$
文献[10]	$3m$	C_m^2	$o(1)$
文献[11]	$4m$	$2m$	$o(\lg n)$

6 结束语

本文在深入研究 Sybil 攻击特点和 ZigBee 无线网络技术的基础上，采用与节点发送功率无关的多径幅值比值设计了“零存储”的链路指纹。在此基础上，提出了信道相干时间估测算法和 GTS 动态申

请算法，实时跟踪信道变化，减少链路指纹测算与比对次数。最后，对方案在实际使用中的安全性进行分析，推导出方案的安全边界条件，并分别设计实验对方案安全性和自适应性进行验证，结果表明，本文方案实现代价较小，而节点识别成功率较高，且对通信环境和节点数量具有较好的自适应性能，有效增强了 ZigBee 网络的安全性能。

参 考 文 献

[1] YEE H C and RAHAYU Y. Monitoring parking space availability via ZigBee technology[J]. *International Journal of Future Computer and Communication*, 2014, 3(6): 377–380. doi: 10.7763/IJFCC.2014.V3.331.

[2] TSENG H W, LEE Y H, YEN L Y, *et al*. ZigBee (2.4 G) wireless sensor network application on indoor intrusion detection[C]. 2015 IEEE International Conference on Consumer Electronics, Taipei, China, 2015: 434–435.

[3] DOUCEUR J R. The Sybil attack[C]. 1st International Workshop on Peer-to-Peer Systems, Cambridge, MA, USA, 2002: 251–260.

[4] THAKUR P, PATEL R, and PATEL N. A proposed framework for protection of identity based attack in ZigBee[C]. 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015: 628–632. doi: 10.1109/CSNT.2015.243.

[5] ZHANG Q, WANG P, REEVES D S, *et al*. Defending against Sybil attacks in sensor networks[C]. 25th IEEE International Conference on Distributed Computing Systems Workshops, Columbus, Ohio, USA, 2005: 185–191. doi: 10.1109/ICDCSW.2005.57.

[6] NEWSOME J, SHI E, SONG D, *et al*. The Sybil attack in sensor networks: analysis & defenses[C]. Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, California, USA, 2004: 259–268.

[7] DI PIETRO R, GUARINO S, VERDE N V, *et al*. Security in wireless ad-hoc networks — A survey[J]. *Computer Communications*, 2014, 51: 1–20.

[8] ZENG K, GOVINDAN K, and MOHAPATRA P. Non-cryptographic authentication and identification in wireless networks[J]. *IEEE Wireless Communications*, 2010, 17(5): 56–62.

[9] PATWARI N and KASERA S K. Robust location distinction using temporal link signatures[C]. Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking, Montréal, Québec, Canada, 2007: 111–122. doi: 10.1145/1287853.1287867.

[10] LIU Y and NING P. Enhanced wireless channel authentication using time-synched link signature[C]. INFOCOM 2012 Proceedings IEEE, Orlando, FL, USA, 2012: 2636–2640.

[11] XIAO L, GREENSTEIN L J, MANDAYAM N B, *et al*. Channel-based detection of Sybil attacks in wireless networks[J]. *IEEE Transactions on Information Forensics and Security*, 2009, 4(3): 492–503. doi: 10.1109/TIFS.2009.2026454.

[12] JAKES W C and COX D C. Microwave Mobile Communications[M]. Hoboken, NJ, USA, Wiley-IEEE Press, 1994: 1–69.

[13] HE F, MAN H, KIVANC D, *et al*. EPSON: enhanced physical security in OFDM networks[C]. IEEE International Conference on Communications, Dresden, Germany, 2009: 1–5. doi: 10.1109/ICC.2009.5198999.

[14] 华苏重, 葛丽嘉. 相对时延在码片内的多径分离[J]. 通信学报, 2001, 22(2): 42–48.
HUA Suchong and GE Lijia. Separation of sub-chip multipath components[J]. *Journal on Communications*, 2001, 22(2): 42–48.

[15] 罗炬锋, 邱云周, 付耀先, 等. 研究片内多径分离技术在基于 RSSI 定位中的应用[J]. 电子与信息学报, 2011, 33(4): 891–895. doi: 10.3724/SP.J.1146.2010.00780.
LUO Jufeng, QI Yunzhou, FU Yaoxian, *et al*. Research on separation of subchip multipath components for RSSI-based location application[J]. *Journal of Electronics & Information Technology*, 2011, 33(4): 891–895. doi: 10.3724/SP.J.1146.2010.00780.

[16] AKHLAQ M and SHELTAMI T R. Rtsp: an accurate and energy-efficient protocol for clock synchronization in wsns[J]. *IEEE Transactions on Instrumentation and Measurement*, 2013, 62(3): 578–589.

[17] 郁滨, 周伟伟. ZigBee 同频攻击检测抑制模型研究[J]. 电子与信息学报, 2015, 37(9): 2211–2217. doi: 10.11999/JEIT141395.
YU Bin and ZHOU Weiwei. Co-channel attack detection and suppression model for ZigBee network nodes[J]. *Journal of Electronics & Information Technology*, 2015, 37(9): 2211–2217. doi: 10.11999/JEIT141395.

[18] 罗海军, 彭卫东. 整体最小二乘法在精同步中的应用[J]. 计算机测量与控制, 2014, 22(7): 2291–2294.
LUO Haijun and PENG Weidong. Application of total least squares in precise synchronization[J]. *Computer Measurement & Control*, 2014, 22(7): 2291–2294.

郁 滨： 男，1964 年生，教授，博士生导师，主要研究方向为无线网络安全和视觉密码.

黄美根： 男，1990 年生，硕士生，研究方向为 ZigBee、无线网络安全.

黄一才： 男，1985 年生，讲师，研究方向为信息安全技术.