传感器网络中基于时钟偏移的伪造节点攻击检测技术

焦程波

(1. 信息工程大学，郑州 450002; 2. 西南电子电信技术研究所，成都 610041)

摘　要： 研究一种基于时钟偏移的传感器网络中伪造节点攻击被动式检测技术。以节点之间的时钟同步数据作为输入，构建相对发送/接收时间差序列，提取数据发送源的相对时钟偏移。在此基础上，提出了 DSNA(detect spoofed node attack)算法，通过检测相对发送/接收时间差序列异常识别伪造节点攻击，进一步在确定了攻击模式的基础上，对不同节点所发送的同步数据进行分类并提取时钟偏移作为指纹识别出伪造节点。在真实传感器网络环境下对检测技术进行了验证，结果表明该方法可以在被动方式下，快速准确地实现对伪造节点攻击的检测和伪造节点的识别。

关键词： 伪造节点攻击; 时钟偏移; 指纹; 时钟同步

中图分类号： TP311　　**文献标志码：** A　　**文章编号：** 1001-3695(2011)11-4291-05

doi:10.3969/j.issn.1001-3695.2011.11.079

Research of spoofed node detection in wireless sensor network based on clock skew

JIAO Cheng-bo

(1. *Information Engineering University*, *Zhengzhou* 450002, *China*; 2. *Southwestern Institute of Electronics & Telecommunication*, *Chengdu* 610041, *China*)

Abstract: This paper stadied a novel passive spoofed node attack detection technique in wireless sensor network (WSN). It estimatedn node's relative send/receive time difference series and clock skew by analyzing time synchronization data transmitted in WSN. Based on the analysis of attack pattern, it proposed DSNA algorithm by checking the relative send/receive time difference series to detect spoofed node attack, and then it could identify spoofed node by using clock skew as its fingerprint. The test under real environment shows that this technique can passively detect spoofed node attack and identify spoofed node quickly with high precision.

Key words: spoofed node attack; clock skew; fingerprint; time synchronization

传感器节点是物联网中重要的组成部分，其通过无线通信方式实现物理层的互联。传感器节点通常部署于无人值守且不可控制的非安全环境下，因此不仅面临传统无线网络中传输信息被窜改与泄露的威胁，节点信息还面临被攻击者通过物理手段获取的威胁，因此，传感器节点的身份认证是物联网安全领域的核心技术之一[1~5]。攻击者获取了节点信息之后可以通过伪造节点身份发动攻击，与互联网中伪造 IP 源地址攻击相类似，而目前还没有在传感器节点身份验证方面形成统一的解决方法、相关理论和体系结构。

据笔者所知，目前还没有其他研究工作利用时钟偏移针对传感器网络环境下的伪造节点攻击进行分析。本文通过分析同步数据相对发送/接收时间差序列和节点时钟偏移，研究了传感器节点中存在的伪造节点攻击检测技术。

不同的物理设备拥有彼此各异的细微特征，利用细微特征差异对设备进行识别是当前网络安全和计算机取证等领域中的一种重要技术手段[6,7]。与其他类型网络中的节点相比，无线传感器网络节点受到低功耗、低带宽和链路失效等问题的制约，其节点身份认证方法需要拥有简单快速等特性。基于此，考察当前具有代表性的传感器节点同步协议，本文通过被动分析节点之间传输的时钟同步数据完成对伪造节点的识别，不需要主动发送数据，降低了识别方法的应用限制。并分别通过检测相对发送/接收时间差序列异常和节点指纹变化情况完成对伪造节点攻击和伪造节点的识别。

本文简要介绍了传感器网络中节点身份识别的相关方法和存在的问题；并对伪造节点攻击进行了分析，比较了本领域的相关工作，分析了传感器节点的时钟同步协议及机制和时钟偏移估算。针对不同的伪造节点攻击模式，提出了伪造节点识别方法 DSNA。DSNA 结合伪造节点所发送的时钟同步数据特征，通过检测节点之间发送/接收时间差序列异常和时钟偏移变化情况完成对伪造节点的快速准确识别，并在真实环境下进行了相关测试。

1　伪造节点攻击介绍

在 Berkeley Mica/Mica2 motes 系统[8] 上搭建了伪造节点攻击测试平台，因为时钟偏移代表个体特征，所以测试节点均为相同的软硬件配置，避免软硬件配置造成的差异，图 1 中展示了伪造节点攻击拓扑结构。

图 1 中共有 6 个节点，其中节点 1、2、3、4 为普通节点(标示为 N1、N2、N3、N4)，节点 5 为检测节点(标示为 M1)；F1 为伪造节点，其通过伪造 N1 的 ID 与其他节点进行通信，因此不能通过 ID 等信息完成对 N1 和 F1 节点的分类。同时，为了尽可能真实地模拟 N1 发送数据的特征，F1 与 N1 部署于相同的

收稿日期：2011-04-06；修回日期：2011-05-17

作者简介：焦程波(1982-)，男，博士研究生，主要研究方向为网络测量与网络安全(crusie@yahoo.com.cn)。

位置区间。与IEEE 802.11下的伪造节点攻击相同,伪造传感器节点攻击存在多种模式,即按照N1和F1所发送同步数据是否共存,可以将伪造节点攻击分为以下两类: a) N1与F1发送的同步数据不共存; b) N1与F1发送的同步数据共存。

因此在完成对伪造节点攻击识别后,需要进一步完成对攻击模式的识别,根据攻击模式来区分源自不同节点的数据。

2 相关工作

当前的设备时钟因为制造工艺的影响,彼此之间存在时钟偏移现象,即运行频率上难以达到准确的同步。在文献[6,7,9]中分别提出利用时钟偏移识别不同网络环境中的设备,下面分别对其进行简要介绍和分析。

通过观测和统计不同设备的时钟偏移结果,Tadayoshi等人在文献[6]中提出利用时钟偏移完成对互联网中设备的识别,其分别通过提取ICMP、TCP、IP和HTTP数据报中的时间戳完成其发送源时钟偏移的估算,并对时钟偏移的稳定性和可分性进行了统计。结果显示,不同设备之间的时钟偏移存在较大的偏差,且单个设备的时钟偏移稳定,满足了作为识别设备参数的基本要求。在文献[9]中,Steven提出利用时钟偏移与环境的映射关系,深层次挖掘匿名网络中服务器属性,为识别匿名设备提供了一种技术手段。在文献[7]中,Suman等人分析了IEEE 802.11网络中接入点AP(access point)所发送时间戳的变化规律,提出利用时钟偏移完成对伪造AP的识别,测试结果显示,其可以有效完成伪造AP的识别。

本文通过分析和测试发现,无论N1和F1所发送的同步数据是否共存,均可以通过检测同步数据的相对发送/接收时间差序列异常完成对攻击的识别。在文献[7]中虽然提出了攻击模式存在两种情况,但并没有给出区分攻击模式的方法,其对第一种攻击模式下伪造节点攻击和伪造节点的识别技术是建立在任何一段同步数据均来自同一节点的前提下。而在实际情况中,该模式下任意一段攻击数据可能分时段存在源自不同节点的同步数据中,因此同样需要对数据进行区分,否则可能导致误判。在N1与F1发送的同步数据共存情况下,文献[7]采用两种算法完成对数据的分类,其中算法2从数据集合中学习得到阈值,在此基础上算法1利用阈值完成对不同节点所发送数据的区分。本文提出直接通过比较不同算法对时钟偏移的估算结果,完成对混合数据的区分,降低了该模式下区分算法的运算复杂度。在完成同步数据的区分后,根据时钟偏移估算结果可以完成对各个节点真实身份的识别。

相较于其他网络环境,无线传感器节点之间具有较小的传输噪声。RBS(reference broadcast synchronization)、TPSN(timing synch protocol for sensor networks)和FTSP(flooding time synchronization protocol)等协议是当前无线传感器网络中具有代表性的同步协议[10~13],其主要通过定时发送同步信息或交换同步数据进行节点之间的同步操作。FTSP协议是使用时间戳进行同步操作的代表性协议,其通过发送MAC层时间戳由同步源向其他节点泛洪广播时间同步信息,以确保准确的时钟同步。

3 时钟偏移估算

节点时钟同步过程中,接收方在接收到同步信息后,其系统时间将因为校时操作而发生突变,如果不对系统时间突变进行处理将无法正确估算时钟偏移。针对这个问题,结合无线传感器节点之间同步信息发送间隔时间较短和时钟突变较小的特点,采用文献[14,15]中的方法检测接收方的时钟突变现象,消除接收方时钟突变对时钟偏移估算的影响。下文中的时钟偏移估算及其相关分析均是建立在消除了时钟突变现象的基础上,以接收方时钟作为基准时钟,完成对节点之间相对时钟偏移的估算和分析。

设当前捕获了$N+1$个同步数据报,那么第i个同步数据相对于第1个同步数据的相对接收时间差Rr_i和发送时间差Rs_i满足式(1)。

$$\begin{cases} Rr_i = r_i - r_0 \\ Rs_i = H(s_i - s_0) \end{cases} \quad i \in [1, N] \tag{1}$$

其中:r_0和s_0分别代表第1个同步数据报的捕获和发送时间;r_i和s_i分别代表第i个同步数据捕获和发送时间;H代表时间戳计数值与时间值之间的频率对应关系。如果时间戳代表真实时间,则$H=1$,否则时间戳存在四舍五入的量化误差。令cs代表发送方和接收方之间的固定相对时钟偏移(clock skew),在噪声影响较小的情况下,结合式(1)由时钟偏移的定义[6,16~18],可以得到式(2)。

$$cs = \frac{\mathrm{d}\Delta_i}{\mathrm{d}Rr_i}, \Delta_i = Rr_i - Rs_i, i \in [1, N] \tag{2}$$

其中:Δ_i代表第i个同步数据报的相对发送/捕获时间差。令Δ序列代表同步数据报的相对发送/捕获时间差序列。由式(2)可知,cs即为Δ时间序列斜率,因此cs的估算转换为Δ时间序列斜率的拟合问题。

与FTSP协议不同,在其他一些时钟同步协议中不进行同步时间信息的传输,但其在固定时间点中进行同步,此种情况下,根据同步信息发送间隔时间段固定的特点可以准确获取Rs_i,该情况下采用式(2)同样可以完成其时钟偏移的估算。

文献[9~13]中对数据的发送、传输和接收过程进行了分解。同步数据在传输过程中可能会遇到传输信道冲突和节点资源调度繁忙等引入的随机噪声,其将在一定程度上影响cs的估算结果。对于RBS和TPSN等协议,其受到中断处理和解码处理等随机噪声的影响较大。在正常运行环境下,累积随机噪声较小,但在非正常运行环境下(如在中断处理禁止、处理资源紧张和外部环境改变),累积随机噪声较大。由式(2)可知,累积随机噪声较大时将对cs的有效准确估算造成影响。因此需要在一定的约束条件下抑制噪声,完成对cs的准确估算,即拟合Δ_i时间序列斜率。下面对含噪Δ序列中cs的估算问题进行分析。

文献[6~7,16~19]中分别提出了包括分段中值拟合、分段最小拟合、线性规划拟合(linear programming fitting, LPF)和最小方差拟合(least squares fitting, LSF)等在内的多种具有代表性的时钟偏移估算方法,不同的估算方法在不同的约束条件下可对斜率进行线性拟合,其中LPF是当前主要的时钟偏移拟合算法。

设α_{lpf}和β_{lpf}为LPF的拟合斜率和拟合截距,结合式(2)可得到如式(3)的表达式:

$$\begin{cases} \Delta_i \geqslant \alpha_{lpf} Rr_i + \beta_{lpf} \\ \min\{\frac{1}{N}\sum_{i=1}^{N}(\Delta_i - \alpha_{lpf} Rr_i - \beta_{lpf})\} \end{cases} \tag{3}$$

由式(3)可知,α_{lpf}和β_{lpf}为Δ序列的下限拟合斜率和截距。令ε_i代表Δ_i中携带的噪声,其计算过程为

$$\varepsilon_i = \Delta_i - cs \cdot Rr_i \tag{4}$$

令 $\varepsilon_{\min}$ 满足 $\varepsilon_{\min}=\min\{\varepsilon_k, k\in[0,N]\}$。综合式(3)(4)可知，当 $\forall i,j\in[1,N]$，$\varepsilon_i,\varepsilon_j$ 满足 $\varepsilon_i\neq\varepsilon_j\neq\varepsilon_{\min}$ 时，$\alpha_{lpf}\neq cs$。同理当 ε 序列满足式(5)时，可以得到 $\alpha_{lpf}=cs$，式(5)如下：

$$\exists i,j\in[0,N], i\neq j, \varepsilon_i=\varepsilon_j=\varepsilon_{\min} \tag{5}$$

设 p 代表 $\forall i\in[1,N]$，ε_i 满足 $\varepsilon_i=\varepsilon_{\min}$ 的概率，则对于 ε 序列来讲，其中存在 k 个值满足 $\varepsilon_i=\varepsilon_{\min}$ 的概率可以表示为 $C_N^k p^k(1-p)^{N-k}$。综合式(5)可得到 $\alpha_{lpf}=cs$ 的概率为

$$1-(1-p)^N-C_N^1 p(1-p)^{N-1} \tag{6}$$

由式(6)可知，对于含噪 Δ 序列中 cs 的估算问题，通过延长 Δ 序列，可以提高 α_{lpf} 估算结果的准确性，在下面的实际测试过程中如果不特别说明，一段数据的长度均大于等于 900 s。

Berkeley Mica/Mica2 motes 环境下 FTSP 时间戳精度可以达到微秒级，同时其采用包括在 MAC 层打时间戳等机制较好地降低了时钟偏移估算中的包括位置误差在内的其他误差[8,13,20]，满足了在较短时间内准确完成时钟偏移估算的基本条件。

在下文中如果不特别说明，均在 FTSP 协议环境下利用 LPF 完成时钟偏移的估算。估算过程中，普通节点采用随机方式发送时间戳到检测节点，检测节点在接收到时间戳后完成时钟偏移估算，结果均以百万分之一(percentage per million，PPM)为单位。

4　伪造节点识别技术 DSNA

本节介绍了伪造节点识别技术 DSNA，其首先检测伪造节点攻击，进一步对攻击模式进行区分，根据不同攻击模式完成对源自不同节点同步数据的区分；最后完成对伪造节点的识别。

4.1　伪造节点攻击检测

在第一类攻击模式下，F1 和 N1 各自发送的时间戳 ts^F 和 ts^N 不共存，因此来自相同 ID 节点的 Δ 序列如式(7)所示。

$$\Delta=\{(Rr_1,\Delta_1^N),\cdots(Rr_i,\Delta_i^N),(Rr_i,\Delta_{i+1}^F),\cdots\} \tag{7}$$

其中：Δ_i^N 和 Δ_i^F 分别为来自 N1 和 F1 的相对时间差。由式(7)可知，如果 F1 没有与 N1 进行时钟同步，那么 Δ 序列将出现明显的突变现象，如图 2 所示。

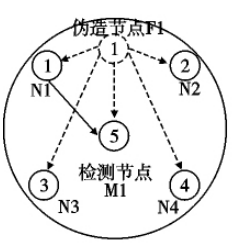

图1　伪造节点攻击拓扑结构

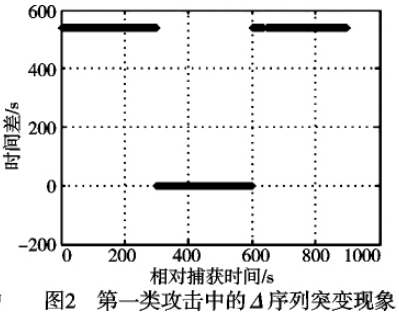

图2　第一类攻击中的 Δ 序列突变现象

如果 F1 同步于 N1 的时钟，将不会出现图 2 中的 Δ 突变现象，但是因为不同设备时钟偏移不同，将导致 Δ 序列的斜率发生变化，如图 3 所示。

在第二类攻击中，N1 与 F1 的时间戳共存且交叉出现，因此来自相同 ID 节点的 Δ 序列如式(8)所示。

$$\Delta=\{\cdots(Rr_i,\Delta_i^N),(Rr_i,\Delta_{i+1}^F),(Rr_i,\Delta_{i+2}^N)\cdots\} \tag{8}$$

在图 4、5 中分别展示了第二类攻击中的 Δ 序列异常情况。

图 2～5 分别展示了伪造节点攻击造成的 Δ 序列异常情况，使用 LPF 和 LSF 分别拟合了各种异常情况下的时钟漂移估算结果，如表 1 所示。

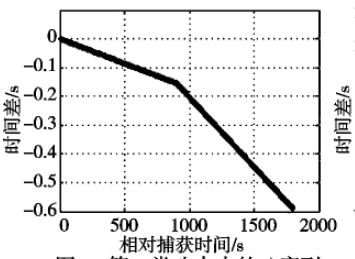

图3　第一类攻击中的 Δ 序列斜率变化现象

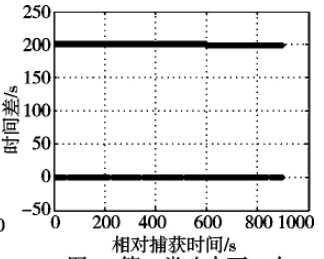

图4　第二类攻击下N1与F1未同步情况

表 1　Δ 序列异常情况下 LPF 与 LSF 结果比较

图标号	α_{lpf}	α_{lsf}	$\lvert\alpha_{lpf}-\alpha_{lsf}\rvert$
2	-35.2	-10 772.4	10 737.2
3	-328.7	-416.8	88.1
4	-172.8	41.8	214.6
5	-483.5	-468.7	14.8

由表 1 可以发现，在 Δ 序列异常情况下，α_{lpf} 和 α_{lsf} 的差值远远大于正常情况下的偏差(1PPM)，因此可以通过检测 $\lvert\alpha_{lpf}-\alpha_{lsf}\rvert$ 的变化情况完成对伪造节点攻击的检测。

比较图 2～5 可以发现，通过检测突变点是否存在可以完成对攻击类型的判断。在第一类攻击模式下，通过检测突变点可以完成对 Δ 序列的分类。在第二类攻击模式下，虽然 Δ 序列不存在突变点，但通过 α_{lsf} 可以完成对来自不同节点的 Δ 序列进行分类。设 k 为 Δ 序列发送源的个数，对 Δ 序列的数据分类为 k 未知情况下的数据分类问题，因此首先需要完成对 k 的正确计算。

4.2　数据的分类

在第一类攻击模式下，因为不同节点所发送的同步数据不共存，$\lvert\alpha_{lpf}-\alpha_{lsf}\rvert$ 异常由不同节点所发送的 Δ 混在一起所造成。针对这个现象，本文引入了分段算法 FSCLL(first segmentation algorithm by comparing LPF and LSF)，其按照 Rr_i 递增的顺序通过逐步递归比较时间段 Δt 内不同 Δ 之间的 $\lvert\alpha_{lpf}-\alpha_{lsf}\rvert$，完成对 Δ 序列的分段，直到其满足 $\lvert\alpha_{lpf}-\alpha_{lsf}\rvert\leqslant 1$ ppm，而每一段分离出数据序列的开头点即为异常点。以下是 FSCLL 的伪代码。

```
procedure FSCLL
input: Δ,k, SegHash   //segHash 代表分段哈希数值组,K 代表分段个数
begin
k = 1
push(SegHash{k},Δ1)   //Δ1 放入到 segHash 中的第 1 个分段数组中
for i = 2 to N
push(SegHash{k},Δi)   //Δi 放入到 segHash 中的第 k 个分段数组中
αlpf = LPF(SegHash{k})   //估算 segHash 中的第 k 个分段数组的 LPF 斜率
αlsf = LSF(SegHash{k})   //估算 segHash 中的第 k 个分段数组的 LSF 斜率
if abs(αlpf - αlsf) >2ppm
pop(SegHash{k})   //退出 segHash 中的第 k 个分段数组的栈顶值
k + +   //发现异常点,建立新的分段
push(SegHash{k},Δi) //Δi 放入到 segHash 中的第 k 个分段数组中
```

end //end for if
end// end for for
Output: SegHash //输出分段哈希数组

采用 FSCLL 算法对图 2、3 的结果进行了分段，如图 6、7 所示。

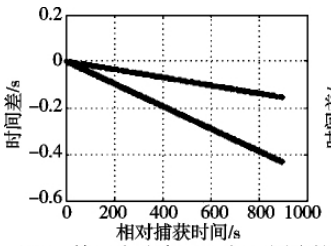

图5 第二类攻击下N1与F1同步情况

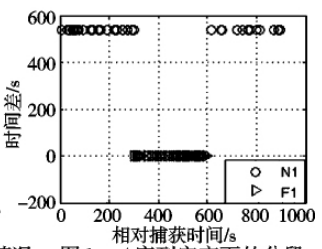

图6 Δ序列突变下的分段

在第二种攻击模式下，由图 4、5 可以发现，N1 和 F1 均以较高的频率发送同步数据，且传输过程中噪声影响很小，令 α_{lpf}^{N1}、α_{lsf}^{N1}、α_{lpf}^{F1}和 α_{lsf}^{F1}分别代表其对应的 LPF 和 LSF 估算结果，由表 1 的统计结果可以得到式(9)：

$$\alpha_{lpf}^{N1} \approx \alpha_{lsf}^{N1}, \alpha_{lpf}^{F1} \approx \alpha_{lsf}^{F1} \tag{9}$$

由 LSF 的定义得到 α_{lsf}的表达式为

$$\alpha_{lsf} = \frac{\sum_{i=1}^{N}\left(\left(Rr_i - \frac{1}{N}\sum_{i=1}^{N}Rr_i\right)\left(\Delta_i - \frac{1}{N}\sum_{i=1}^{N}\Delta_i\right)\right)}{\sum_{i=1}^{N}\left(Rr_i - \frac{1}{N}\sum_{i=1}^{N}Rr_i\right)^2} \tag{10}$$

令 cs^{N1}和 cs^{F1}分别代表 N1 和 F1 的时钟偏移，同时假设 $cs^{N1} < cs^{F1}$，则由式(9)可以得到：

$$\alpha_{lsf}^{N1} < \alpha_{lsf}^{F1} \tag{11}$$

因为 Δ 序列属于 N1 和 F1 共存的混合模式，在式(2)的基础上将来自节点 F1 的序列值 Δ_i^{F1} 替换为来自节点 N1 的序列值 Δ_i^{N1}，得到 N1 的对应 Δ^{N1} 序列，且其估算的时钟偏移值为 α_{lpf}^{N1}。

由式(10)可以得到：

$$\alpha_{lsf} - \alpha_{lsf}^{N1} = \frac{\sum_{i=1}^{N}\left(\left(Rr_i - \frac{1}{N}\sum_{i=1}^{N}Rr_i\right)\left(\Delta'_i - \frac{1}{N}\sum_{i=1}^{N}\Delta'_i\right)\right)}{\sum_{i=1}^{N}\left(Rr_i - \frac{1}{N}\sum_{i=1}^{N}Rr_i\right)^2}$$

$$\Delta'_i = \alpha_{lsf}^{F1}.Rr_i - \alpha_{lsf}^{N1}.Rr_i \tag{12}$$

由式(11)可以得到：

$$\forall i \in [1, N], \Delta'_i \geqslant 0 \tag{13}$$

进一步化简式(12)可以得到式(14)：

$$\alpha_{lsf} - \alpha_{lsf}^{N1} = \frac{\alpha_{lsf}^{F1-N1}\sum_{i=1}^{N}\left(Rr_i - \frac{1}{N}\sum_{i=1}^{N}Rr_i\right)^2}{\sum_{i=1}^{N}\left(Rr_i - \frac{1}{N}\sum_{i=1}^{N}Rr_i\right)^2}$$

$$\alpha_{lsf}^{F1-N1} = \left(\alpha_{lsf}^{F1} - \alpha_{lsf}^{N1}\right) \tag{14}$$

综合式(13)(14)可以得到：

$$\alpha_{lsf} - \alpha_{lsf}^{N1} \geqslant 0 \tag{15}$$

进一步，因为$\{Rr_i, i \in [1, N]\}$为递增数列，可以得到：

$$\alpha_{lsf} - \alpha_{lsf}^{N1} > 0 \tag{16}$$

同理，可证明 α_{lsf}和 α_{lsf}^{F1}满足：

$$\alpha_{lsf} - \alpha_{lsf}^{F1} < 0 \tag{17}$$

综合式(17)(18)可得到：

$$\alpha_{lsf}^{F1} > \alpha_{lsf} > \alpha_{lsf}^{N1} \tag{18}$$

在 F1 与 N1 不同步的情况下，在 Rr_0 时刻伪造节点和真实节点存在时间差，可得到：

$$\beta_{lpf}^{F1} > \beta_{lsf} > \beta_{lpf}^{N1} \tag{19}$$

在 F1 与 N1 同步的情况下，可得到：

$$\beta_{lpf}^{F1} = \beta_{lsf} = \beta_{lpf}^{N1} \tag{20}$$

综合式(19)(20)，可得到：

$$\beta_{lpf}^{F1} \geqslant \beta_{lsf} \geqslant \beta_{lpf}^{N1} \tag{21}$$

综合式(18)(21)可以发现，通过比较 Δ_i 和 $\alpha_{lsf}Rr_i + \beta_{lsf}$完成对 Δ 序列中混杂的 Δ^N 序列和 Δ^F 序列进行分类，在此基础上本文引入了分段算法 SSCLL(second segmentation algorithm by comparing LPF and LSF)，其通过 $\alpha_{lsf}Rr_i + \beta_{lsf}$完成对 Δ^N 和 Δ^F 值的分类：对于 $\forall i \in [1, N]$，如果 $\Delta_i > \alpha_{lsf}Rr_i + \beta_{lsf}$，则其属于 Δ^F 序列；否则，其属于 Δ^N 序列。采用 SSCLL 对图 4、5 中的数据进行的分类，结果如图 8、9 所示。

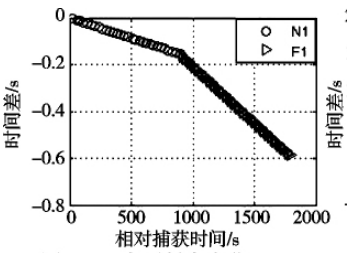

图7 Δ序列斜率变化下的分段

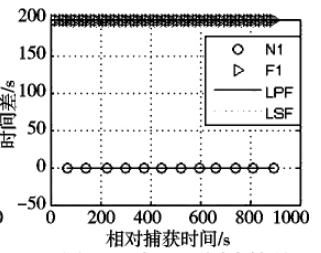

图8 F1与N1不同步情况下序列分类

在图 8、9 的伪造节点攻击中只存在一个伪造节点，在存在多个伪造节点进行攻击时，算法 SSCLL 的数据分类过程中增加迭代过程(比较 α_{lpf}和 α_{lsf}的差异，直到满足$|\alpha_{lpf} - \alpha_{lsf}| \leqslant 2$ ppm；否则继续数据分类操作)可以将多个节点发送的 Δ 数据进行有效分类，其整个过程如图 10 所示。

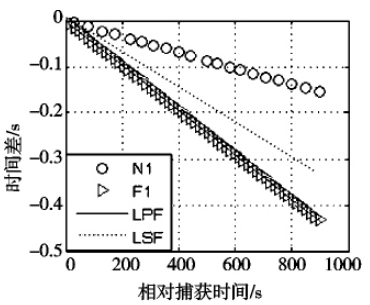

图9 F1与N1同步情况下的Δ序列分类

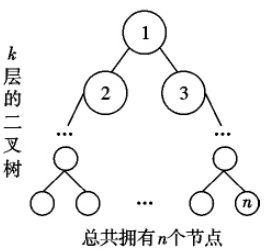

图10 SSCLL分段过程

由图 10 可以知道，二叉树中存在 n 个不同的树叶，说明当前时间差序列中总共混杂了 n 个不同节点的数据。

在完成了对数据的分类之后，在 F 节点中根据时钟偏移估算结果对节点的身份进行识别。

4.3 伪造节点识别技术

在节点接入网络之前先估算其时钟偏移结果，并进行记录，建立指纹数据库以备最后进行伪造节点的识别。DSNA 的运行流程如图 11 所示。

由图 11 可以知道，DSNA 首先通过检测 Δ 序列异常完成对攻击的识别；如果没有检测到攻击，那么估算当前时间段内节点的时钟偏移，并与数据库中的结果进行比较以判断节点的真实身份；在检测到伪造节点攻击后，首先识别攻击模式，使用 4.2 节中的数据分类算法完成对伪造节点和真实节点发送数据的分离，估算每一类数据的始终偏移并与数据库中的结果进行比较以判断节点的真实身份。

5 结束语

本文通过挖掘传感器网络环境下的同步时间信息构建相

对发送/接收时间差序列，并估算时钟偏移。通过检测相对发送/接收时间差序列异常和比较不同节点的时钟偏移，可以完成对伪造节点攻击和伪造节点的快速识别。

在下一步工作中需要结合当前已经提出的同步协议作进一步的时钟偏移测量，并结合不同环境中传感器节点时钟偏移的变化情况进行深入研究。同时可以结合节点运行过程中数据的交互情况，考察其他可以反映节点自身特征的参数。进一步建立更大规模的测试集合，对不同节点时钟偏移的分布性和冲突概率进行估算。

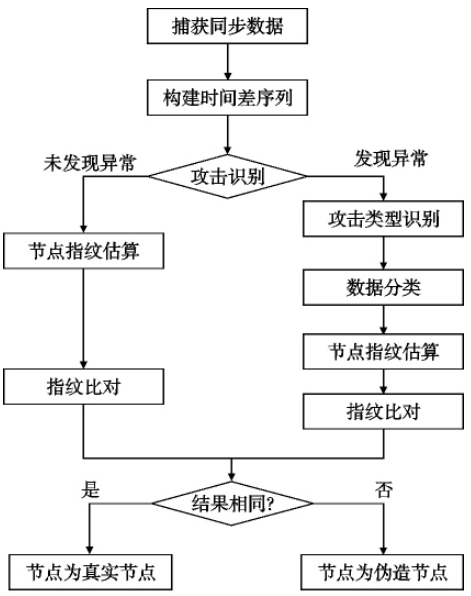

图11　DSNA的运行流程

参考文献：

[1] 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.

[2] OLESHCHUK V. Internet of things and privacy preserving technology [C] //Proc of the 1st International Conference on Wireless Communication，Vehicular Technology，Information Theory and Aero Space & Electronic Systems Technology. [S. l.]：IEEE，2009：336-340.

[3] 李辉，侯义斌，黄樟钦，等. 一种智能攻击模型在 RFID 防伪协议中的研究 [J]. 电子学报. 2009，37(11)：2565-2573.

[4] BUKLEY J. From RFID to the Internet of things pervasive networked systems [R]. Brussels：European Commission，DG Information Society and Media，Networks and Communication Technologies Directorate，2006.

[5] 沈苏彬，范曲立，宗平，等. 物联网的体系结构与相关技术研究 [J]. 南京邮电大学学报，2009，29(6)：1-11.

[6] KOHNO T，BROIDO A，CLAFFY K C. Remote physical device fingerprinting [C] //Proc of IEEE Symposium on Security and Privacy. Los Alamitos，CA：IEEE Computer Society，2005：93-108.

[7] JANA S，KASERA S K. On fast and accurate detection of unauthorized wireless access points using clock skews [C] //Proc of the 14th ACM Sigmobile International Conference on Mobile Computing and Networking. New York：ACM，2008：104-115.

[8] BERKELEY Mica/Mica2 motes [EB/OL]. http：//webs. cs. berkeley. edu/tos/.

[9] MURDOCH S J. Hot or not：revealing hidden services by their clock skew [C] //Proc of the 13th ACM Conference on Computer and Communications Security. New York：ACM，2006：27-36.

[10] ELSON J，GIROD L，ESTRIN D. Fine-grained network time synchronization using reference broadcasts [C] //Proc of the 5th symposium on operating system design implementation. NewYork：ACM，2002：147-163.

[11] GANERIWA S，KUMAR R，SRIVASTAVA M B. Timing synch protocol for sensor networks [C] //Proc of the 1st Conference of Embeded Network Sensor Systems. New york：ACM，2003：138-149.

[12] SYED A，HEIDEMANN J. Time synchronization for high latency acoustic networks [C] //Proc of the INFOCOM. [S. l.]：IEEE，2006：1-12.

[13] MARÓTI M，KUSY B，SIMON G，*et al*. The flooding time synchronization protocol [C] //Proc of 2nd International Conference of Embeded Networked Sensor Systems. New york：ACM，2004：39-49.

[14] 王俊峰. 高速互联网性能测量若干关键技术研究 [D]. 成都：电子科技大学，2004.

[15] WANG Jun-feng，YANG Jian-hua，ZHOU Hong-xia，*et al*. Detecting clock dynamics in one-way delay measurement [J]. Journal of Software，2004，15(4)：584-593.

[16] MOON S B，SKELLY P，TOWSLEY D. Estimation and removal of clock skew for network delay measurements [C] //Proc of the IEEE INFOCOM Conference. New York：IEEE，1999：227-234.

[17] QASIM C，ERCHIN S，KHALID Q. On maximum likelihood estimation of clock offset and skew in networks with exponential delays [J]. IEEE Trans on signal processing，2008，56(4)：1685-1697.

[18] MILLS D L. Network time protocol (Version 3) specification，implementation and analysis，RFC 1305 [R]. 1992.

[19] PAXSON V E，Measurement and analysis of end-to-end Internet dynamics [D]. Berkeley：University of California at Berkeley，1997.

[20] 黎文伟，张大方，谢高岗，等. 基于通用 PC 架构的高精度时延测量 [J]. 软件学报，2006，17(2)：275-284.

(上接第 4269 页)

[10] JOHN B，GEORGE D B，MARK D C. Surviving attacks on disruption-tolerant networks without authentication [C] //Proc of the 8th ACM International Symposium on Mobile Ad hoc Networking and Computing. New York：ACM Press，2007：61-70.

[11] JOSH B，DAVID A M，DAVID B J. A performance comparison of multi-hop wireless Ad hoc network routing protocols [C] //Proc of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking. New York：ACM Press，1998：85-97.

[12] JUN H，AMMAR M H，ZEGURA E W. Power management in delay tolerant networks：a framework and knowledge-based mechanisms [C] //Proc of the 2nd Annual IEEE Communications Society Conference on Sensor and Ad hoc Communications and Networks. 2005：418-429.

[13] KERÖNEN A，OTT J，KARKKAINEN T. The ONE simulator for DTN protocol evaluation [C] //Proc of the 2nd International Conference on Simulation Tools and Techniques. Brussels：ICST，2009：56-74.

[14] MUHAMMAD A，GEORGE M. Characteristics of common mobility models for opportunistic networks [C] //Proc of the 2nd ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks. New York：ACM Press，2007：107-109.