Software Engineering and Applications 软件工程与应用, 2014, 3, 15-21
http://dx.doi.org/10.12677/sea.2014.31003 Published Online February 2014 (http://www.hanspub.org/journal/sea.html)

A Passive Detection Approach of Capture Attacks in WSNs Based on Qualitative Evaluation

Jingbo Li, Guangwei Zhang

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing
Email: dianerliu@yahoo.com.cn

Received: Dec. 4th, 2013; revised: Jan. 3rd, 2014; accepted: Jan. 14th, 2014

Abstract: Since the nodes of WSNs are always deployed on the outside, nodes are easy to be captured. The traditional detection approaches of capture attack can be categorized as approaches based on time of absence and approaches based on passive intrusion detection. The former requires extra communication cost, and the latter needs to carry on the statistical analysis of the whole network signal strength. In this paper, the qualitative and quantitative uncertainty conversion ability of cloud model is used to evaluate the signal strengths among WSN nodes real-time. Normal cloud models are built based on the evaluation. The qualitative judgments of nodes are made, and the capture attacks in WSNs can be detected in time. Simulation results show that, this method can greatly improve the detection accuracy, and that the false alarm rate is low.

Keywords: Wireless Sensor Networks; Capture Attacks; Passive Intrusion Detection; Cloud Model

基于定性评估的 WSN 节点捕获攻击被动检测方法

李晶博，张光卫

北京邮电大学网络与交换技术国家重点实验室，北京
Email: dianerliu@yahoo.com.cn

收稿日期：2013 年 12 月 4 日；修回日期：2014 年 1 月 3 日；录用日期：2014 年 1 月 14 日

摘　要：由于通常部署于外界，WSN 节点易于被敌手捕获。传统捕获攻击的监测方法主要有基于缺席时间的监测及被动入侵检测两类，前者需要额外的通信开销，而后者则需要对网络整体信号强度进行统计分析，对单个节点入侵的识别通常不够敏感。本文利用云模型定性知识与定量数值之间的不确定性转换能力，对 WSN 节点之间通信中信号强度进行实时统计，建立信号强度云模型，得出节点是否遭遇入侵的定性判断，进而对可疑节点一段时间内信号强度进行分析，判断是否遭遇捕获攻击。仿真实验证明，该方法能够较大程度地提高检测的准确度，且误报率较低。

关键词：无线传感器网络；捕获攻击；被动入侵检测；云模型

1. 引言

无线传感器网络(Wireless Sensor Network, WSN)是由播撒在一定范围内的大量传感器节点自组织而成的网络，用以采集目标区域内的环境数据[1]。近年来，WSN 被广泛用于环境的监测和保护、医疗护理、工业检测等多种领域[2]。由于 WSN 本身的开放性，

通常被部署在野外较恶劣的无人值守环境中，因而节点易于被敌手捕获并重新编程，成为恶意节点，对整个网络进行攻击。传统的信息安全技术，通常难以应对 WSN 中的节点捕获攻击[3]。当前对节点捕获攻击较为有效的监测多采取缺席监测方法[4,5]以及被动入侵检测方法[6-12]。

缺席监测方法中，WSN 节点定期向邻居发送额外消息，若邻居一段时间内未回复该消息，则认为该节点被敌手捕获。这种方法通常需要不小的额外通信开销。由于 WSN 通常由廉价的、使用无线方式进行数据传输的传感器节点组成，且节点使用电池供电，能量供应十分有限。频繁的数据通信不仅会耗费网络资源，更会导致节点电量急剧消耗。据统计，WSN 节点传输每 bit 数据耗电量约为执行一条指令耗电量的 1000 倍[13]。

与主动入侵检测不同，WSN 中的被动入侵检测是指检测目标不需要携带任何无线设备，通过分析 WSN 节点之间通信过程中的信号强度实现的入侵检测。由于无线信号在遭遇障碍物、遮挡时，会因散射、反射等情况出现信号减弱的情况，因而，通过分析 WSN 节点之间信号强度的异常情况，即可发现网络中出现的异常情况，从而实现监测。自 2007 年 Youssef 首次提出了 DFL (Device-Free Localization)的概念[6]起，被动入侵检测的研究引起了广泛的重视及全面的研究，Youssef 于 2009 年实现了 DFL 入侵检测系统[7]，Ossi Kaltiokallio[8]对接收信号强度进行了分布式的处理与分析，基于处理结果，实现被动入侵检测，Bojan Mrazovac[9]则采取对信号强度的主成分进行分析的方法，实现被动入侵监测。Dian Zhang[10]等人根据入侵者在一条链路中不同位置对信号强度的不同影响，提出了中点和交叉点算法，通过多条链路的共同作用实现目标的入侵检测。Jie Yang[11]提出了 GREEK 算法，实现被动入侵检测。Ahmed E. Kosba[12]则利用利用统计学的知识，通过异常检测技术实现入侵判断。然而，以上基于被动检测的方法需要对网络进行整体评估，需要建立全局检测机制，检测多基于对信号强度的期望、标准差等统计数据，较难适应传感器网络的自组织特征。本文提出了一种针对单个节点的入侵检测方法，节点接收数据时使用云模型对信号强度进行实时统计，并实现实时的节点被动入侵检测，使用该方法，对节点捕获攻击入侵进行了监测，仿真结果表明该方法能及时监测出节点捕获攻击，有较高的检测率及较低的误报率。

后文组织如下：第 2 部分给出问题模型，介绍云模型并完成信号强度的建模，第 3 部分给出基于云模型的 WSN 被动入侵检测方法，并分析算法的复杂性。第 4 部分给出仿真实验的设计、实验和结果分析，最后总结并指出下一步的工作。

2. 问题模型

在 WSN 的被动入侵检测问题中，被检测对象无需安装无线设备，而被检测对象通常会对 WSN 节点之间的无线传输造成遮蔽，因此，检测过程通常通过对 WSN 节点之间接收信号强度的统计实现。本节分析了 WSN 节点之间接收信号强度的影响因素，并探讨了现有的几种常见统计方法，并提出了基于云模型的信号强度统计方法。本文的入侵检测方法将在此基础上实现。

2.1. 接收信号强度

WSN 无线传输中，接收信号强度(Received Signal Strength Indication, RSSI)通常受发送端的发射功率、接收端的接受增益、发送距离、遮蔽损耗、测量误差等影响。根据无线信号传输模型[14]，RSSI 有如下公式：

$$\mathrm{RSSI} = P + G - L - 10\beta \log_{10} d - S + v \tag{1}$$

其中，P 为发送端的发送功率，G 为接收端的接受增益，L 为信号功率衰减值，β 为路径衰落指数，d 为发送距离，S 为遮蔽损耗，v 为测量误差。在 WSN 特定两个节点之间，P、G、L、β、d 通常为定值，v 通常为高斯随机数。

正常情况下，若无敌手入侵，WSN 两个节点之间遮蔽损耗通常也为定值，令：

$$base = P + G - L - 10\beta \log_{10} d - S \tag{2}$$

则：

$$RSSI = base + v \tag{3}$$

易知：若 v 为高斯分布，则 RSSI 也为高斯分布。

基于此结论，在 WSN 中，若两节点间接受信号强度出现明显异常，则可能是 G、L、β、d、S 中的一

个或多个出现了变化。在静态 WSN 中，β、d 不会发生改变，若用户未对 G、L 进行人为设置的改变，可认为 S 出现了异常变化，即：出现了异常遮蔽损耗，由此可判断有敌手入侵网络。

传统技术中对接收信号强度的异常情况判断方法多对信号强度的期望或标准差进行统计[7]，基于此，本文提出了一种算法简单，对于异常变化敏感度更高的统计方法——基于云模型的 RSSI 统计方法。

2.2. 基于云模型的统计方法

云模型的概念于 1995 年，由我国工程院院士李德毅教授正式提出[15]。至今云模型已成功应用到数据挖掘、智能控制、图像处理等众多领域[16,17]。

云模型是用语言值描述的某个定性概念与其数值表示之间的不确定性转换模型。以云的数字特征——期望 Ex，熵 En 和超熵 He 表示语言值的数学性质，记做 C (Ex, En, He)，称为云的特征向量。逆向云算法是一种特殊的统计方法，可以实现对定量值进行统计，从而对其进行不确定性评估。常用的逆向云算法为无确定度的逆向正态云算法，记做 bwdcloud，算法如下：

算法 1：无确定度的逆向正态云算法[15]。

输入：N 个云滴 $\{x_1, x_2, \cdots, x_N\}$

输出：这 N 个云滴表示的定性概念的期望值 Ex、熵 En 和超熵 He

步骤：

step1：根据 xi 计算这组数据的样本均值 $\bar{X} = \frac{1}{N}\sum_{i=1}^{N} x_i$，一阶样本绝对中心矩 $\frac{1}{N}\sum_{i=1}^{N}\left|x_i - \bar{X}\right|$，样本方差 $S^2 = \frac{1}{N-1}\sum_{i=1}^{N}\left(x_i - \bar{X}\right)^2$；

step2：Ex 的估计值为 $E\hat{x} = \bar{X}$；

step3：En 的估计值为 $E\hat{n} = \sqrt{\frac{\pi}{2}} \times \frac{1}{N}\sum_{i=1}^{N}\left|x_i - E\hat{x}\right|$；

step4：He 的估计值为 $H\hat{e} = \sqrt{S^2 - E\hat{n}^2}$。

易知，$(ex, en, he) = bwdcloud\left(\{x_1, x_2, \cdots, x_N\}\right)$，此算法时间复杂度为 $o(N)$。

使用逆向云算法，对信号强度进行统计，不仅可以反映信号强度的整体水平，还能对信号强度的离散程度及不确定程度进行全面评估，通过与信号强度云的比较，易于发现 RSSI 的异常变化。

2.3. 基于云模型的统计方法评估

云模型能够全面描述数据的整体情况、离散程度、以及不确定度，在具有高度不确定性的系统中，使用云模型的方法评估更为全面。

由于正态分布广泛存在于自然现象、社会现象、科学技术以及生产活动中，在很多系统中，数据的分布往往呈现正态分布的特点。中心极限定理从理论上阐述了产生正态分布的条件，是正态分布普适性的理论基础。

然而在强调正态分布的地位同时，必须指出许多随机现象不能用正态分布来描绘。如果决定随机现象的因素单独作用不是均匀地小，某些因素间存在相互依赖，那么就不能够严格符合正态分布的产生条件，不构成正态分布或者只能用正态分布来近似处理。概率论用联合分布来处理这类情况，但联合概率分布的确定非常复杂，难以实际应用。

正态云可以看成是一种由放宽正态分布的产生条件，或由正态分布扩展的泛正态分布，泛正态分布在一定程度上描述了这类随机性。云模型用独立参数超熵，来衡量偏离正态分布的程度，这种处理方法比单纯用正态条件分布更为宽松，同时比联合分布简单，易于表示和操作。

当超熵 $He = 0$ 时，所有云滴都分布在高斯曲线上，云退化为正态分布，称 $He = 0$ 为云的正态点.从这个意义上说，正态分布是云的特例；当 He 逐渐增大的时候，云滴开始离散，云滴的凝聚性变差了；$He = En/3$ 时，由于 y2 的指数趋向负无穷大，函数值趋于 0，云图开始雾化。正态云由正态分布变化为雾的过程如图 1 所示。

以两组数据为例，说明云模型统计方法的科学性。

另集合 a = {1,3,1,3,1,3}，b = {1,1,2,2,2,4}，两组数据的期望均为 2，标准差均为 1，使用期望、标准差对数据进行统计，无法识别两组数据的区别。使用逆向云模型对两个数据进行统计，记为 C_a，C_b，计算可得，$C_a = (2, 1.25, 0.61)$，$C_b = (2, 0.84, 0.71)$，集合 a、集合 b 云滴的分布如图 2 所示。

根据两个云的数值可以看出，两组数据整体水平一样，第一组数据离散度较高，不确定度较低，第二组数据离散度较低，而不确定度较高。根据图 2，集合 a 的云滴分布比较离散，然而还可以看出整体接近

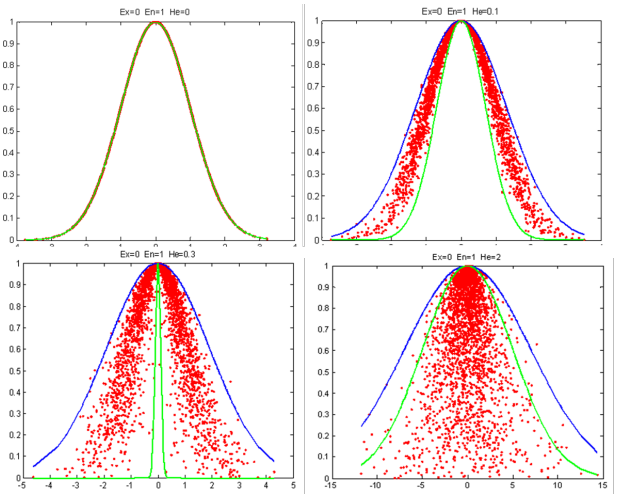

Figure 1. Different status of normal cloud
图 1. 云的雾化过程

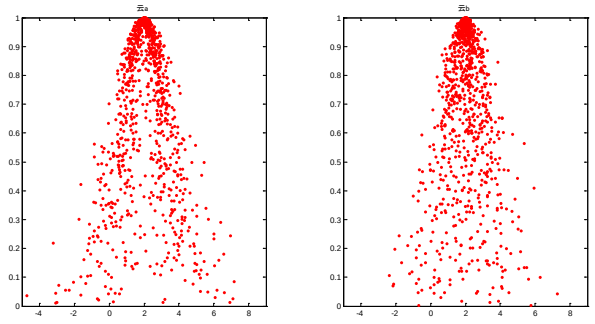

Figure 2. Drop distribution of set a and b
图 2. 集合 a、集合 b 云滴分布

正态分布，而集合 b 的云滴则出现很明显的雾化现象。在第二组数据中，数值 4 相比平均数据偏差较大，属于离群点，云模型的描述方法，能够对数据分布情况进行定性评估，进而有效识别异常的数据。

3. 基于云模型的 WSN 被动入侵检测方法

3.1. 检测条件

在 WSN 中，若每次接收到信号，都对信号进行监测，将给 WSN 节点带来较多的计算开销。因此，本文采取对一段时间内节点信号强度进行逆向云模型统计的方法，当信号强度低于某一阈值，才进行入侵检测。

使用逆向云模型，将最近 n 次接收到某节点的信号强度进行统计，得到信号强度云 $C_{\mathrm{RSSI}}(ex,en,he)$，接收到新的数据时，通过与信号强度云的比较，判断是否进行入侵检测。

在正态云模型中，不同区域内的云滴群对定性概念的贡献不同，其出现的概率也不同。其中，68%的云滴在 $(ex-en,ex+en)$ 内，95%的云滴在 $(ex-2en,ex+2en)$ 内，因此信号强度低于 $ex-en$ 或信号强度低于 $ex-2en$ 时进行入侵检测，可使监测次数降低 68%或 95%，不同区域内的云滴群对定性概念的贡献[15]如图 3 所示。本文方法中，将该条件设置为 $ex-en$。

3.2. 入侵判断

在正态云模型中，超熵是熵的不确定性度量，而熵则是期望的不确定性度量。若信号强度云为：$C_{\mathrm{RSSI}}(ex,en,he)$，则信号强度分布的标准差 σ 符合正态分布 $N(en,he^2)$，根据正态分布的特性，$\sigma\in(en+he,\infty)$ 的概率为 16%左右，而信号强度 $\mathrm{RSSI}\in(-\infty,ex-\sigma)$ 的概率也为 16%左右，因此，信号强度 $\mathrm{RSSI}\in(-\infty,ex-en-he)$ 的概率约为 2.56%，连 n 两次信号强度 $\mathrm{RSSI}\in(-\infty,ex-en-he)$ 的概率约为 $0.0256^n\times100\%$。

根据以上分析，当连续两次信号强度低于 $ex-en-he$，或者两个邻居节点收到信号强度均低于 $ex-en-he$ 时，可判断节点遭遇捕获攻击。

3.3. 检测算法

根据以上分析设计基于云模型的被动检测算法(Cloud-based Passive Intrusion Detection for WSN，简称 CPID)：

算法 2：基于云模型的被动检测算法(CPID)。

输入：目标节点信号强度序列 $\{\mathrm{RSSI}_1,\mathrm{RSSI}_2,\cdots\}$，缓存窗口大小 n

输出：节点遭遇攻击时间点 t

步骤：

step1：节点为目标节点开辟大小为 n 的缓存；

step2：存储来自目标节点信息的信号强度；

step3：缓存存满后执行逆向云算法，统计信号强度云 $C_{\mathrm{RSSI}}(ex,en,he)=bwdcloud(\{\mathrm{RSSI}_1,\cdots,\mathrm{RSSI}_n\})$；

step4：清空缓存，并存储之后信号强度；

step5：比较信号强度是否达到监测条件；

step6：if ($\mathrm{RSSI}_i\le ex-en$)；

step7：广播该节点可疑；

step8：每个邻居执行监测，if($\mathrm{RSSI}_i\le ex-en-he$)，发送该节点异常时间点至汇聚节点；

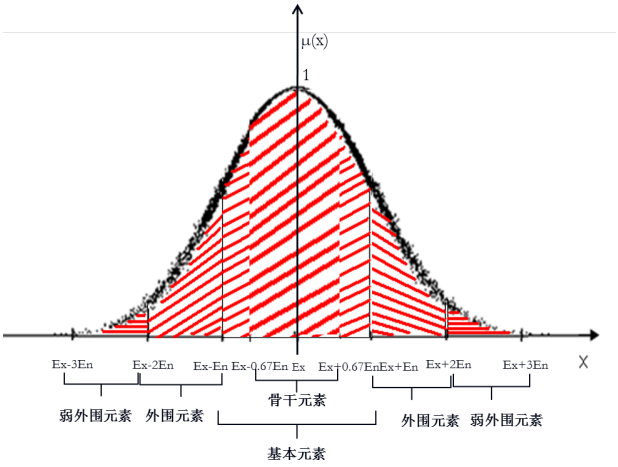

Figure 3. **Contribution of drops in different area**
图 3. **不同区域内的云滴群对定性概念的贡献**

step9：汇聚节点收到节点异常消息两次以上，则判断该节点遭遇攻击，并在网内广播该节点遭遇入侵消息；

step10：循环执行 step2~step9；

该算法采取多个邻居联合实时检测目标节点的思路，通过该算法，可及时发现节点遭遇异常入侵情况，实时性较好。

3.4. 整体开销

综合分析该算法，可知该算法共包括三方面的开销。

通信开销：该算法在节点出现异常时需要发送异常消息至汇聚节点，汇聚节点需要广播该节点异常。若节点遭遇攻击次数为 num，则该算法通信开销为 $O(num)$。

存储开销：该算法执行中，每个节点需要为每个邻居开辟固定大小的缓存，若每个节点平均邻居数为 m，每个邻居缓存大小为 n，则该算法存储开销为 $O(mn)$。

计算时间开销：该算法执行中，每个邻居每 n 次数据需要执行一次逆向云算法，而逆向云算法计算时间开销为 $o(n)$，因而，该算法整体计算时间开销为 $O\left(\frac{mn}{n}\right)=O(m)$。

综上，该算法通信开销较低，有一定存储开销，计算开销较低，由于 WSN 网内通常通信资源较为紧张，节点计算能力有效，因此该算法能够满足 WSN 对于算法的额外要求，适用于实际的 WSN 应用环境。

4. 仿真实验

4.1. 实验建立

实验使用的无线节点由 SoC zigbee 芯片 CC2530、传感器、PCB 天线、电源电路以及 JTAG 调试接口组成。如图 4 所示。

本文使用四个节点进行模拟实验，任意两个节点之间可以相互发送消息，布局如图 5 所示。

在该场景中，各节点首先按照 TDMA 机制，进行数据发送，每个节点将采集到的数据进行广播，其他节点均可对该节点信号强度进行采集与分析。

节点捕获攻击将在 4 号节点发生，用户由门进入，并将 4 号节点取走，在此过程中，节点 1、节点 3 接收到节点 4 信号强度将受到影响。根据仿真实验情况，在 matlab 中进行多次攻击模拟，并分析结果。

4.2. 实验结果

模拟对 4 号节点的 10~200 次入侵，并对各种入侵次数均进行 100 次模拟实验，使用基于云模型的被动入侵检测算法对入侵行为进行监测，统计整体检测率及误报率，得到图 6 和图 7 结果。

分析实验结果可知，当入侵次数增多时，检测率会略有下降，这是由于入侵次数增多，会使得信号强度云波动增大，因此，在再次出现信号强度异常时，会导致漏报情况出现。而误报率始终为 0，这是由于随着入侵次数的增多，入侵行为与正常行为之间的区别更为明显，因此始终不会有正常情况被认为是异常情况而误报。

4.3. 对比分析

对基于云模型的方法，与文献[4]中提出的基于缺席监测方法 FSD 以及文献[6]中提出的基于信号强度期望的 DFL-均值方法进行综合比较，若整个网络中有 n 个节点，对这些节点共发生了 num 次入侵，则三种方法的综合性能比较如表 1 所示。

易知，使用基于云模型的 WSN 节点捕获攻击被动监测方法相比其他方法，监测率较高，误报率较低，且需要的额外通信开销很低，具有较好的性能与较高的实用性。

5. 结语

本文对 WSN 中无线传输的信号强度进行了建模，

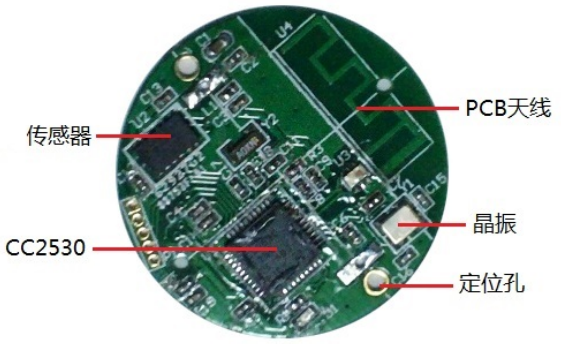

Figure 4. Node of wireless sensor network
图 4. 实验使用的 WSN 节点

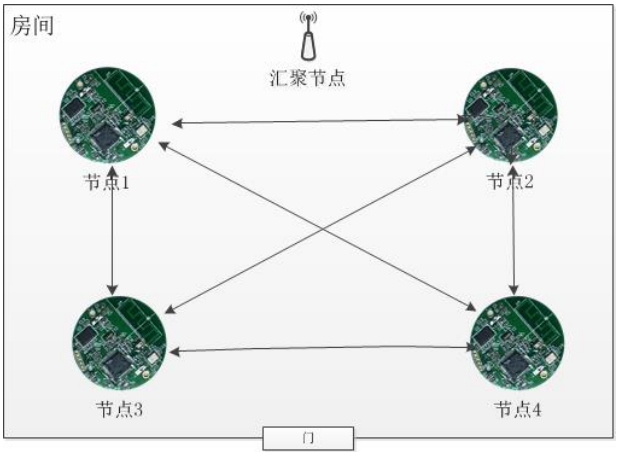

Figure 5. Scenario of test
图 5. 实验场景设计

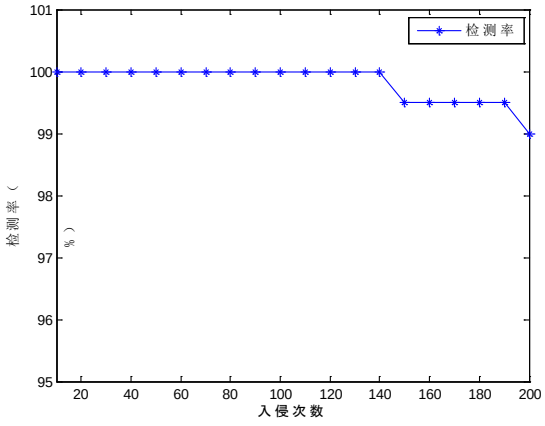

Figure 6. Map between intrusion quantity and efficiency
图 6. 检测率与入侵次数关系

通过分析，提出了正常情况下，信号强度应服从高斯分布的结论，基于此结论，使用云模型对节点接收信号强度进行统计，计算出信号强的期望、熵、超熵，并在云模型自身特性的基础上，定义了检测条件，大大降低了通信开销；定义了入侵的判断方法，提高了

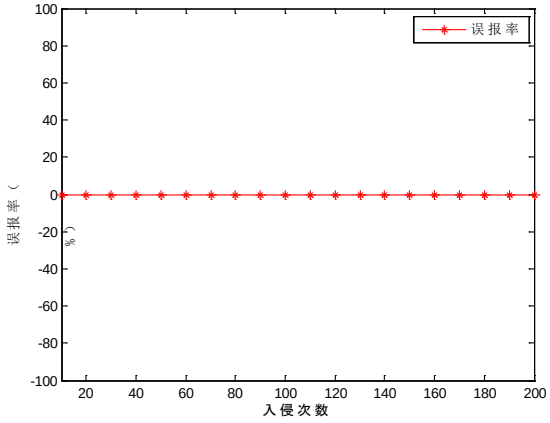

Figure 7. Map between intrusion quantity and misstatement rate
图 7. 误报率与入侵次数关系

Table 1. Comparisons of performance
表 1. 与其他方法的综合性能对比

方法	监测目标	通信开销	检测率(%)	误报率(%)
CPID	节点	O (num)	99~100	0
FSD	节点	O (n)	99~100	0~10
DFL-均值	整个网络	O (n)	60~70	20~30

监测的精度。实验结果及算法的综合性能比较与分析证明了该方法具有较高的检测率，较低的误报率，较小的开销，较敏感的入侵发现，在实际的 WSN 应用中有较高的可用性。

基金项目

本文受国家自然科学基金(61272521)，教育部博士点基金(20110005130001)资助。

参考文献 (References)

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., et al. (2002) Wireless sensor networks: A survey. *Computer Networks*, **38**, 393-422.

[2] 孙利民, 李建中, 陈渝, 等 (2005) 无线传感器网络. 清华大学出版社, 北京.

[3] Perrig, A., Stankovic, J. and Wagner, D. (2004) Security in wireless sensor networks. *Communications of the ACM*, **47**, 53-57.

[4] Ding, W., Laha, B., et al. (2010) First stage detection of compromised nodes in sensor networks. *IEEE Sensors Applications Symposium* (*SAS*), Limerick, 23-25 February 2010, 20-24.

[5] Ding, W., Yu, Y., et al. (2010) Distributed first stage detection for node capture. *IEEE GLOBECOM Workshop* (*GC Wkshps*), Miami, 6-10 December 2010, 1566-1570.

[6] Youssef, M., Mah, M. and Agrawala, A. (2007) Challenges: Device-free passive localization for wireless environments. *Proceedings of the* 13*th Annual ACM International Conference on Mobile Computing and Networking*, Montreal, 9-14 Septem-

ber 2007, 222-229.

[7] Moussa, M. and Youssef, M. (2009) Smart devices for smart Environments: Device-free passive detection in real environments. *IEEE International Conference on Pervasive Computing and Communications* (*PerCom* 2009), Galveston, 9-13 March 2009, 1-6.

[8] Kaltiokallio, O. and Bocca, M. (2011) Real-time intrusion detection and tracking in indoor environment through distributed RSSI processing. *IEEE* 17*th International Conference on Embedded and Real-Time Computing Systems and Applications* (*RTCSA*), Toyama, 28-31 August 2011, 61-70.

[9] Mrazovac, B., Bjelica, M.Z. and Kukolj, D. (2012) System design for passive human detection using principal components of the signal strength space. *IEEE* 19*th International Conference and Workshops on Engineering of Computer Based Systems* (*ECBS*), Novi Sad, 11-13 April 2012, 164-172.

[10] Zhang, D., Ma, J., Chen, Q.B. and Ni, L.M. (2007) An RF-based system for tracking transceiver-free objects. 5*th Annual IEEE International Conference on Pervasive Computing and Communications*, White Plains, 19-23 March 2007, 135-144.

[11] Yang, J., Ge, Y., et al. (2010) Performing joint learning for passive intrusion detection in pervasive wireless environments. *Proceedings of IEEE INFOCOM*, San Diego, 14-19 March 2010, 1-9.

[12] Kosba, A.E., Saeed, A. and Youssef, M. (2012) RASID: A robust WLAN device-free passive motion detection system. *IEEE International Conference on Pervasive Computing and Communications*, Lugano, 19-23 March 2012, 180-189.

[13] Crossbrow Inc. (2003) MPR—Mote processor radio board user's manual.

[14] 詹杰, 刘宏立, 刘述钢 (2011) 基于 RSSI 的动态权重定位算法研究. *电子学报*, **1**, 82-88.

[15] 李德毅, 杜鹢 (2005) 不确定性人工智能. 国防工业出版社, 北京.

[16] 吕辉军, 王晔, 李德毅, 等 (2003) 逆向云在定性评价中的应用. *计算机学报*, **8**, 1009-1014.

[17] 宋远骏, 李德毅, 杨孝宗, 等 (2000) 电子产品可靠性的云模型评价方法. *电子学报*, **12**, 68, 74-76.