

基于移动 Sink 的 WSN 安全数据收集方法

苗春雨¹, 范渊¹, 李晖², 葛凯强¹, 张小孟¹

(1. 杭州安恒信息技术股份有限公司, 浙江 杭州 310051;

2. 西安电子科技大学网络与信息安全学院, 陕西 西安 710126)

摘要: 由于目前基于移动 Sink 的 WSN 数据收集方法存在网络攻击检测率不高、内存开销大等问题, 导致网络较易受到网络攻击且难以被实际应用。针对该问题, 提出一种基于移动 Sink 的 WSN 安全数据收集方法, 利用能量感知的凸壳算法, 识别数据收集点, 使用椭圆加密算法 (ECC) 为网络内的所有节点生成密钥, 通过 ElGamal 算法实现节点身份和消息的认证, 使用支持向量机 (SVM) 识别网络攻击类型。仿真实验结果表明, 所提出的安全数据收集方法在攻击检测率、内存开销以及数据包投递率方面都表现出较好的性能。

关键词: WSN; 移动 Sink; 数据收集; ElGamal 算法

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021013

Secure data collection method of WSN based on mobile Sink

MIAO Chunyu¹, FAN Yuan¹, LI Hui², GE Kaiqiang¹, ZHANG Xiaomeng¹

1. Hangzhou DAS-Security Information Technology Co., Ltd., Hangzhou 310051, China

2. School of Cyber Engineering of Xidian University, Xi'an 710126, China

Abstract: At present, WSN data collection method based on mobile Sink has some problems, such as low detection rate of network attack and large memory cost, which makes the network vulnerable to network attack and difficult to be applied in practice. To solve this problem, a secure data collection WSN method of WSN based on mobile Sink was proposed, which used convex hull algorithm of energy perception to identify data collection points, used elliptic encryption algorithm (ECC) to generate key for all nodes in the network, used ElGamal algorithm to realize node identity and message authentication, and used support vector machine (SVM) to identify network attack types. The simulation results show that the proposed secure data collection method has good performance in attack detection rate, memory overhead and packet delivery rate.

Keywords: WSN, mobile Sink, data collection, ElGamal algorithm

收稿日期: 2020-05-25; 修回日期: 2020-07-14

通信作者: 张小孟, aaron.zhang@dbappsecurity.com.cn

基金项目: 国家自然科学基金重点项目 (61732022)

Foundation Item: The Key Program National Natural Science Foundation of China (61732022)

论文引用格式: 苗春雨, 范渊, 李晖, 等. 基于移动 Sink 的 WSN 安全数据收集方法[J]. 网络与信息安全学报, 2021, 7(1): 121-129.

MIAO C Y, FAN Y, LI H, et al. Secure data collection method of WSN based on mobile Sink[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 121-129.

1 引言

无线传感器网络 (WSN, wireless sensor network) 是一种由大量的无线传感器节点组成, 并以无线、自组织的形式构成的通信网络。无线传感器网络应用广泛且常被部署于环境恶劣、无人值守的环境之中, 如污染物监测、战场监视和火山监控等^[1-2]。

通过静态的 Sink 进行网络通信通常会导致能耗热点问题, 距离 Sink 越近的节点转发的数据越多, 消耗能量就越大, 从而造成网络能耗不均衡、降低了网络生存时间。文献[3-5]分别提出了通过移动 Sink 节点进行解决的方案, Sink 节点的移动减少了消息传输的跳数, 并将高负载任务均衡至更多的传感器节点, 从而网络能耗更加均衡。为了减少网络的总能耗, 采用占空比控制传感器节点的状态 (如工作、休眠和空闲), 系统通过某些条件 (如时间、节点的剩余能量和邻居节点数等) 控制节点状态的转换, 从而提高节点的连通性和覆盖范围, 进而延长网络寿命^[6]。由于网络在应用的过程中常遭到网络攻击, 遭到攻击时将导致网络关键数据被窃取、修改或者删除, 因此在数据传输时需要对网络进行数据认证, 并且识别出对应的恶意节点, 从而提高网络数据收集时的安全性^[7-8]。

在移动 Sink 研究方面, Mario 等^[9]提出通过移动 Sink 进行概率性地访问传感器节点进行数据收集的方法, 利用静态节点的 3 种状态 (发现、休眠和数据传输), 在发现阶段检测 Sink 节点的到达, 从移动 Sink 接收信标帧使节点进入数据传输状态, 当节点没有要传输的数据包时, 节点切换至休眠状态。该方法通过静态节点周期性地收集数据, 因此在一定程度上降低了网络能耗, 但未考虑数据传输的安全性。Lai 等^[10]提出一种通过控制节点占空比降低移动 Sink 无线传感器网络能耗的方法, 节点使用状态服务判断 Sink 节点是否到达, 未获得 Sink 节点信息的节点处于脱机状态, 节点根据从邻居节点接收到的信标帧进行状态转换, 并在每个唤醒时隙中发送信标数。由于该方法需要时刻监听移动 Sink 广播的消息, 因此节点消息复杂度较高。Tabibi 等^[11]针对移动

Sink 网络内查找最佳数据收集节点难的问题, 提出基于粒子群优化的选择算法 (PSOBS)。通过应用粒子群算法网络找到最佳或接近最佳的数据收集节点, 该方法在吞吐量和网络能耗方面表现出较好的性能, 但数据丢包率较高。Restucciaf 等^[12]提出一种新颖的基于群智能的传感器选择算法 (SISSA), 该算法优化网络寿命并满足了预定义的 QoS 约束, 但该方法未考虑数据传输时的安全问题。

在移动 Sink 的无线传感器网络安全研究方面, Rasheed 等^[13]针对移动 Sink 网络在基本的概率和 q-composite 密钥预分配方案中, 攻击者通过捕获部分节点获得密钥造成数据安全性的问题, 提出了一个 3 层通用框架, 允许使用任何成对密钥预分配方案作为基本组件。为进一步降低静态节点复制攻击的损失, 在框架中加强了传感器节点与静态访问节点之间的认证机制, 该框架在节点复制攻击方面具有较高的性能, 但对于其他类型的网络攻击检测率较低。Conti 等^[14]提出一种安全拓扑维护协议 (Sec-TMP), 该协议不需要任何底层路由, 只需通过一跳通信就能很好地实现对贪睡攻击 (snooze attack)、睡眠剥夺攻击 (sleep deprivation attack) 和网络替代攻击 (network substitution attack) 的检测。由于 TMP 协议不依赖路由协议, 因此端到端延迟和能耗等性能指标取决于移动 Sink 的运动方式, 由于保存了令牌, 因此该协议具有较高的内存开销。Rajeswari 等^[15]提出一种基于时隙的安全节能拓扑维护协议 (Secs-TMP), 该协议克服了网络能量和存储空间有限的问题。在每个时隙期间只允许少量的节点处于活动状态, 当与时隙关联的计时器到期, 节点进入选举状态。在工作状态时节点通过对称密钥与移动 Sink 进行身份认证, 将认证通过的数据发送至 Sink 节点。当有足够多的工作节点时, 将当前节点切换为睡眠状态, 结果表明 Secs-TMP 协议能够很好地抵抗常见的网络攻击。但由于认证、数据交换以及移动 Sink 的频繁访问导致数据加密时内存开销大。

综上所述, 目前基于移动 Sink 的 WSN 数据收集方法存在网络攻击检测率不高、数据加密时内存开销大等问题, 因此很难实际应用于无线传

传感器网络的数据收集之中。针对该问题, 本文提出了一种基于移动 Sink 的 WSN 安全数据收集方法(SDCM, a secure data collection method of WSN based on mobile Sink), 该方法通过椭圆曲线加密(ECC)为网络内的所有节点生成密钥, 利用 ElGamal 进行消息认证, 最后使用 SVM 对网络数据进行训练, 确定剩余能量阈值, 实现攻击类型的分类。实验结果表明, 该方法在攻击检测率、内存开销以及数据包投递率方面都表现出较好的性能。

2 网络模型与相关假设

2.1 网络模型

本文采用平面网络架构, 网络内节点同构, 网络模型如图 1 所示。普通节点采集网络数据, 并将数据发送给对应的数据收集节点, 数据收集节点将数据转发至合法的移动 Sink, 在移动 Sink 端进行节点身份和网络数据的认证, 并识别出网络攻击的类型。

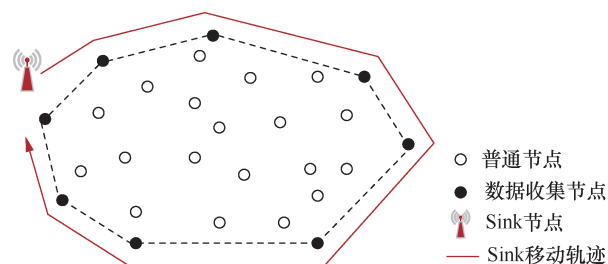


图1 网络模型
Figure 1 Model of network

2.2 相关假设

假设 1 网络内节点随机部署, 部署后节点位置通过 GPS 或者网络定位方法获得。

假设 2 传感器节点在部署前已预加载了公钥和私钥, 恶意节点部署于合法节点之后。

假设 3 网络内的普通节点和数据收集节点的总数量为 N , 且具有相同的初始能量 E_0 。

3 数据收集方法设计

SDCM 首先查找出数据收集节点, 然后根据数据收集节点的位置确定 Sink 节点的移动路径, 接着利用改进的 ElGamal 算法进行节点身份认证并收集合法节点数据, 最后利用支持向量机

(SVM) 对网络进行训练, 确定剩余能量阈值, 实现攻击类型分类。

3.1 网络初始化

网络初始化过程如图 2 所示, 首先选择网络内任一节点作为发起节点(n_s), 发起节点 n_s 向网络内的所有节点(如节点 n_1 、 n_2) 广播位置请求消息(LocReq), 接收到请求的传感器节点回应自身的位置信息(LocRep), 接着发起节点利用文献[16]提出的基于能量感知的凸壳算法找出网络内的所有数据收集节点, 数据收集节点的查找利用了 Jarvis 算法^[17]并考虑了节点的剩余能量, 因此查找出的数据收集节点较为合理。数据收集节点确定之后, 发起节点 n_s 将数据收集节点的信息广播至网络内的所有节点和移动 Sink。网络内普通传感器节点广播 HELLO 消息, 识别最近的数据收集节点以确定跳数, 并与最近的数据收集节点关联进行数据传输。

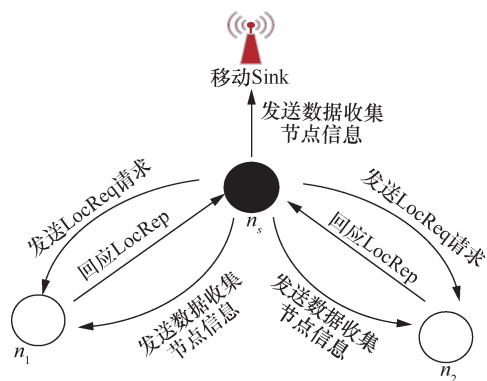


图2 网络初始化
Figure 2 Initiation of network

3.2 确定移动 Sink 路径

首先建立网络区域直角坐标系, 网络内节点通过定位方法获取自身坐标。Sink 节点活动于网络外围, 移动路径如图 1 所示, 移动情况如式(1)所示。

$$\left((X_i^s, Y_i^s), V, T\right)_i \in C_n \quad (1)$$

其中, (X_i^s, Y_i^s) 表示移动 Sink 的位置; V 表示 Sink 的移动速度; T 表示认证成功后在数据收集节点附近进行数据收集时暂停的时间; C_n 表示所有数据收集节点。

为了提高网络的生命周期, 应尽可能地将网

络能耗降到最小, 实现能耗 E 的最小化, 即 $\text{Min } E$ 。

在实现能耗 E 的最小化的同时需要满足式(2)、式(3)和式(4)的条件。

$$E_{C_{n_i}} \leq E_0, \forall C_{n_i} \in N \quad (2)$$

$$\text{Hop}_{ij} \rightarrow \sum_i \min(C_{n_i}), \forall i \in N \quad (3)$$

$$\text{Data}_j = \sum_{j \in C_n} \text{flow}_{ji} \quad (4)$$

式(2)表明数据收集节点的能量是有限的, 应小于节点的初始能量, 当 $E_{C_{n_i}} \rightarrow 0$ 时, 应将其最近的邻居节点当作新的数据收集节点; 式(3)表示普通节点将距离自身跳数最短的数据收集节点作为数据的接收方。式(4)表示将数据收集节点 C_{n_i} 的数据传输给移动 Sink 时的数据量。

定义 1 Sink 的移动轨迹长度 d 由网络内两个连续数据收集节点之间的欧几里得距离的总和进行估算, 如式(5)所示。

$$d = \sum_{i=1}^{N_{C_n}-1} \sqrt{(X_i - X_{i+1})^2 + (Y_i - Y_{i+1})^2} \quad (5)$$

其中, C_n 表示数据收集节点数量

定义 2 Sink 节点的覆盖率 C_{rate} 由每次访问的数据收集节点个数与数据收集节点总数之比确定, 如式(6)所示。

$$C_{\text{rate}} = \frac{N_{\text{cn_cur}}}{N_{\text{cn}}} \quad (6)$$

其中, $N_{\text{cn_cur}}$ 表示每次访问的数据收集节点个数。

3.3 安全数据收集

传感器节点在部署之前, 移动 Sink 基于椭圆加密算法^[18]为网络中的所有节点生成公钥和私钥。对于有限域 $y^2 = x^3 + ax + b \bmod p$ 上的基点 $G_b(x, y)$, 其中 a, b 是椭圆曲线参数, p 是一个大质数且不为 0。生成密钥过程为: 首先随机产生一个数 P_r , 使 $P_r \in [1, n-1]$, 其中 n 是基点 G_b 的阶数。接着计算 $Q_p = P_r \cdot G_b$, 因此节点的公钥为 Q_p , 私钥为 P_r 。

将获得的公钥、私钥和移动 Sink 标识符同时加载到所有的传感器节点中, 当查找到数据收集节点之后, 移动 Sink 与数据收集节点通信进行数

据的收集, 认证成功后实现数据的传输。其中消息认证过程采用 ElGamal 算法^[19]实现。

当节点收集到网络内的数据时, 生成数字签名并附上消息 M , 发送给数据收集节点, 实现过程如下:

(1) 传感器节点产生一个随机数 K_s , 其中 $K_s \in [1, n-1]$, n 为一个质数;

(2) 计算 $R = x \bmod n (0 < x < p)$, x 随机产生;

(3) 计算 $h_a \leftarrow \text{SHA-1}(M, R)$, SHA-1 表示 160 位哈希函数, l 表示哈希的最左位;

(4) 计算 $S_i = R \cdot K_s \cdot h_a + K_s \bmod n$, 如果 $S_i = 0$, 算法转到步骤 (2);

(5) 传感器节点将消息 M 和数字签名 (R, S_i) 同时发送给数据收集节点。

移动 Sink 以随机的时间间隔访问数据收集节点, 并发送请求数据 (Req), 其参数包括移动 Sink 的 ID (N_{id})、时间戳 (T_s)、数字签名、唯一编号 (U_n) 和访问次数 (V_n)。移动 Sink 与数据收集节点之间的安全数据通信过程如图 3 所示。

当数据接收节点接收到 Sink 发送的请求数据 (Req) 后, 首先检查时间戳 T_s 判断消息是否最新, 接着验证移动 Sink 的真实性, 防止恶意节点伪装成移动 Sink 攻击网络。数据接收节点验证移动 Sink 的过程如下。

(1) 检查 N_{id} 是否与移动 Sink 相同。

(2) 检查 V_n 的值是否大于以前的访问次数, 即新 V_n 大于旧 V_n 。其中访问次数 V_n 的值保存在每个数据收集节点的计数器中, 在一个周期内每进行一次成功的数据传输, 就将对应的 V_n 增加 1, 每个数据收集节点的 V_n 值不一定相等。

(3) 检查唯一编号 (U_n) 是否与移动 Sink 的唯一编号相同。

(4) 最后检查移动 Sink 的签名 (R, MS) 。

当初始身份验证成功后, 表示该移动 Sink 是可信的。接着数据收集节点将网络内节点采集的源数据、消息 M 及其关联的数字签名发送到移动 Sink, 接收到消息 M 之后移动 Sink 验证节点身份, 实现步骤如算法 1 所示。算法 1 中的 C_E 表示相关能量参数; E_{cn} 表示数据收集节点的当前剩余能量。

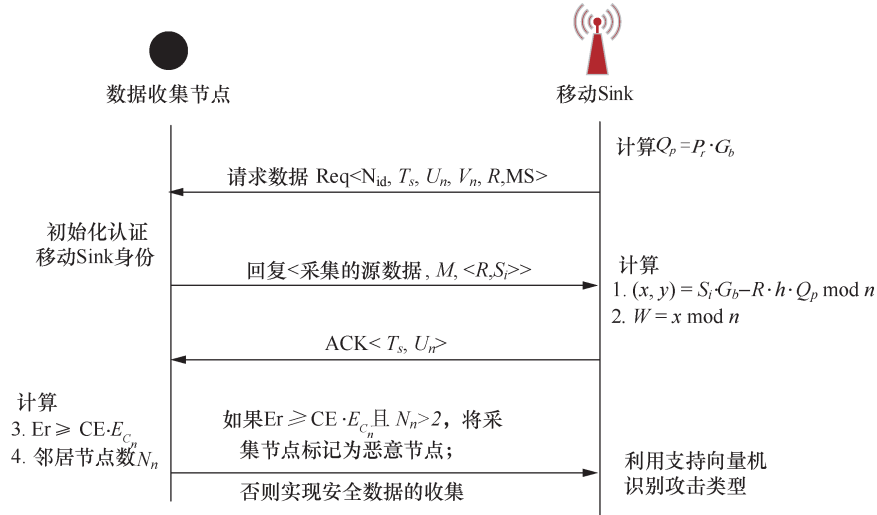


图3 移动 Sink 与数据收集节点之间的安全数据通信过程

Figure 3 Process of security data communication between Sink and collection node

算法1 移动 Sink 验证节点身份

输入 网络内节点采集的源数据、消息 M 及其关联的数字签名

输出 收集数据；识别网络攻击类型

1) 判断 R 和 S_i 的值是否处于范围 $[1, n-1]$ ，

如果不是则该数字签名无效；

2) 计算 $h_a \leftarrow \text{SHA-1}(M, R)$ ；

3) 计算 $X = (x, y) = S_i G_b - R \cdot h \cdot Q_p \bmod n$ ；

4) if $X = O$, then

5) 则拒绝该签名；

6) else

7) 计算 $W = x \bmod n$ ；

8) if $W = R$, then

9) 接收数据收集节点的签名，并将编号 U_n 和时间戳 (T_s) 作为 ACK 进行回复；

10) else

11) 丢弃消息 M ，并通知数据收集节点存在受损节点；

12) 数据收集节点获得采集节点的剩余能量 E_r ；

13) if $E_r \geq C_E \cdot E_{C_n}$ & 采集节点的邻居节点数 $N_n > 2$, then

14) 利用支持向量机识别攻击类型，并将该采集节点标记为恶意节点；

15) 数据收集节点将恶意节点的信息广播到其他数据收集节点以及网络内的其他普通

节点；

16) else

17) Sink 接收采集节点的消息，实现安全数据的收集；

18) end

4 攻击类型检测

网络攻击类型多样，主要有睡眠剥夺攻击 (sleep deprivation attack)、修改攻击 (modification attack)、嗜睡攻击 (snooze attack) 和网络替代攻击等。网络攻击中恶意节点的类型不同其能耗也有所差异，基于此理论本节使用支持向量机^[20]训练网络，确定剩余能量阈值，识别不同的网络攻击。利用支持向量机对不同场景下的不同攻击类型的日志文件进行训练，确定剩余能量阈值 T_e 。训练的样本数据如式(7)所示。

$$((x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)) \mid x_i \in X, y \in \{-1, 1\} \quad (7)$$

其中， x_i 表示输入； $y=1$ 表示正常， $y=-1$ 表示异常。

线性不可分数据的优化问题如式(8)所示，并受限于式(9)。

$$W(\alpha) = \sum_{i=1}^n \alpha_i - \frac{1}{2} \sum_{i,j=1}^n y_i y_j \alpha_i \alpha_j K(x_i, x_j) \quad (8)$$

$$\sum_{i=1}^n \alpha_i y_i = 0, 0 \leq \alpha_i \leq C \quad (9)$$

其中， $W(\alpha)$ 是拉格朗日函数， α_i 是拉格朗日参

数, C 是拉格朗日系数。

用于训练模型的特征包括节点的剩余能量和邻居节点数, 数据被标记为正常和异常, 其中阈值能量由高能耗节点(数据收集节点)和恶意节点之间的差异共同确定。日志文件训练完成后获得攻击类型检测规则, 将该规则加载到移动 Sink 节点中, 以进行恶意节点检测。移动 Sink 识别不同类型的网络攻击过程如图 4 所示。

5 仿真实验

本文在 i7 处理器、8 GB 内存的计算机上使用 Cooja 模拟器^[21]进行仿真实验。本文主要考察了 SDCM 的攻击检测准确率、节点平均能耗、内存开销、数据包投递率和平均端到端延时。为了体现 SDCM 方法性能的优越性, 实验对比了目前性能较好的两种 WSN 数据收集协议: 基于粒子群优化算法的 WSN 移动 Sink 有效路由协议(PSOBS)^[11]和基于时隙的安全节能拓扑维护协议(Secs-TMP)^[15]。实验采用的网络仿真参数配置如表 1 所示。实验数据均为重复独立实验 50 次的平均结果。

表 1 网络仿真参数配置

Table 1 Configuration of network simulation

参数	值
网络区域	2 000 m×2 000 m
节点通信半径 (R)	50 m
节点初始能量 (E_0)	10 J
实验时间	5 min
数据包产生频率	5 s
移动 Sink 的移动速度 (V)	6 m/s
移动 Sink 的收集停留时间 (T)	10 s
相关能量常数 (C_E)	0.38
移动 Sink 的覆盖率 (C_{rate})	0.3

5.1 攻击检测

攻击检测性能是衡量本方法性能优劣最重要的标准之一, 攻击检测的准确度越高, 表示该方法性能越优。实验时在网络区域内部署 100 个传感器节点, 其中包含 5 个相同攻击类型的恶意节点, 独立重复实验 50 次求取平均值(一轮实验)。每完成一轮实验, 改变不同攻击类型的恶意节点重新实验。实验结果如表 2 所示。

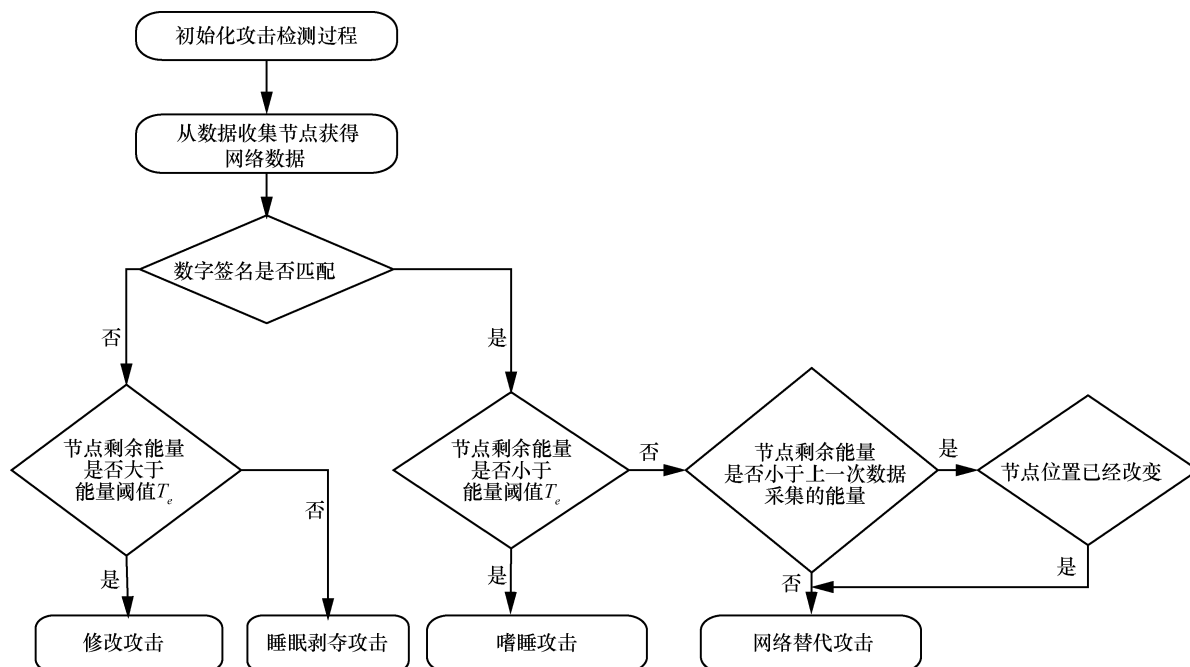


图 4 移动 Sink 识别不同类型的网络攻击过程

Figure 4 Various attack recognition process of Sink node

表 2 攻击检测分析
Table 2 Analysis of attack detection

攻击类型	准确率	错误率
嗜睡攻击	92.4%	7.6%
睡眠剥夺攻击	99.5%	0.5%
网络替代攻击	98.7%	1.3%
修改攻击	98.4%	1.6%

从表 2 可以看出,SDCM 对于睡眠剥夺攻击、网络替代攻击和修改攻击的检测率达到了 98.4% 以上,而对于嗜睡攻击的检测率为 92.4%。这是因为嗜睡攻击识别时涉及剩余能量的计算,存在虚报的可能,即真实节点被标记为恶意节点。当节点没有足够数量的邻居节点时,该节点处于活动状态的时间更长,由于没有状态转换导致较高能耗,因此容易出现识别错误的情况。

5.2 平均能耗

节点平均能耗是衡量网络是否节能的一个标准,节点平均能耗越低表示网络越节能,就越有利于网络的长期生存。本实验采用文献[22]提出的节点能量模型,实验时在网络内部署 8 个恶意节点(每种类型的恶意节点各 2 个),实验分析了不同节点数量对节点平均能耗的影响,实验结果如图 5 所示。

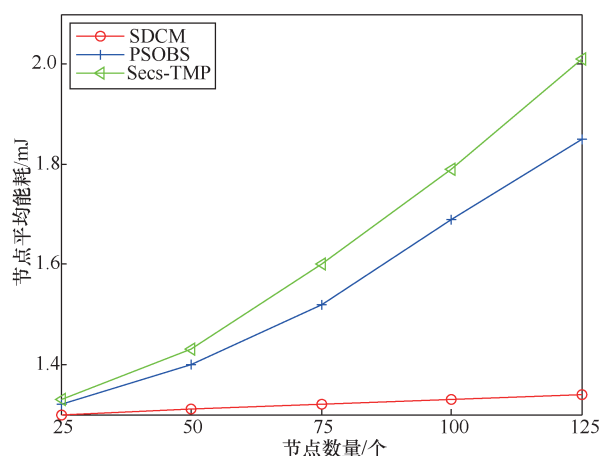


图 5 节点平均能耗
Figure 5 Average energy consumption

从图 5 可知,SDCM 的节点能耗低于 Secs-TMP 和 PSOBS,且随着节点数量的增多 SDCM 节点能耗基本保持不变,而 Secs-TMP 和 PSOBS 的能耗随着网络规模的增大逐渐增大。因为 Secs-TMP 和 PSOBS 需要通过网络内的普通节

点之间进行相互认证以及数据的交换来检测网络攻击,而 SDCM 仅通过数据收集节点和移动 Sink 对节点身份认证,因此减少了相关认证以及数据交换时的能耗。

5.3 内存和时间消耗分析

目前针对无线传感器网络安全数据收集的方法较多,但由于传感器节点的内存和处理能力有限,导致很多方法无法被实际应用于无线传感器网络中,因此内存开销是衡量方法是否可行的重要标准之一。SDCM 采用改进的 ElGamal 方案对网络数据进行安全认证,改进的 ElGamal 方案的内存需求如表 3 所示,其中改进的 ElGamal 方案的各部分执行时间如表 4 所示。

表 3 内存消耗
Table 3 Memory consumption

ROM	RAM		总内存
	Data	Bss	
8 209 byte	16 byte	402 byte	8 627 byte

表 4 时间消耗
Table 4 Time consumption

阶段	时间/ms
生成密钥	60
生成数字签名	41
数字签名认证	89

从表 3 可以得到,ROM 占用 8 209 byte,RAM 占用 418 byte,总内存为 8 627 byte。由于改进的 ElGamal 方案占用了 SDCM 方法大多数的内存,而消耗的内存存在微处理器所能处理的范围之内,因此 SDCM 方法能够实际应用于无线传感器网络之中。从表 4 可以看出实现一个完整的认证过程需要消耗 0.19 s,因此识别效率较高。

5.4 数据包投递率

数据包投递率是衡量网络收集数据是否可靠的重要标准,如果数据包投递率低,可能导致关键数据丢失,从而降低网络收集数据的性能。实验时在网络内部署 8 个恶意节点(每种类型的恶意节点各 2 个),实验分析不同节点数量对数据包投递率的影响,实验结果如图 6 所示。

从图 6 可以看出随着节点数量的增多,SDCM 的数据包投递率一直稳定在较高的水平。这是因为 SDCM 的数据收集节点一直处于工作

状态，并从附近的传感器节点收集数据，而 Secs-TMP 和 PSOBS 方法在移动 Sink 未到达之前处于休眠状态，因此会丢失一部分数据，导致数据包投递率降低。

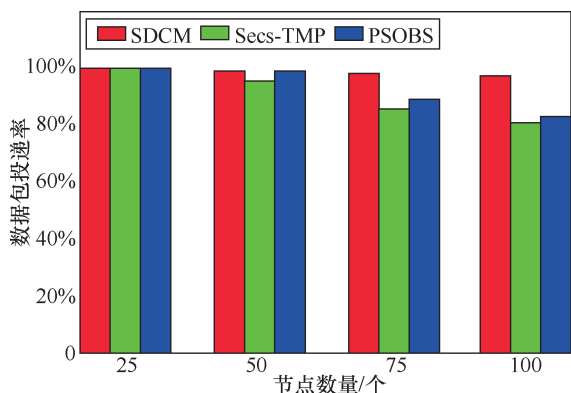


图 6 数据包投递率与节点数量的关系

Figure 6 Relationship of delivery rate of data packet and number of node

5.5 平均端到端时延

平均端到端时延越小表示网络的拥塞率越低，因此一种良好的网络数据收集方法应该具有较低的端到端时延。实验时在网络内随机部署 8 个恶意节点，其中每种攻击类型的恶意节点数为 2，实验分析了不同节点数量与平均端到端时延之间的关系，实验结果如图 7 所示。

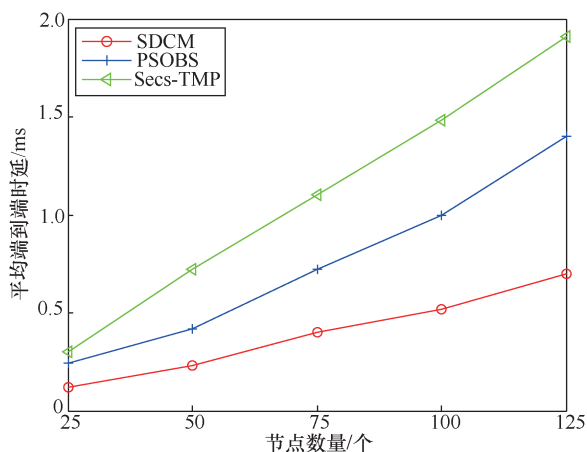


图 7 平均端到端时延与节点数量的关系

Figure 7 Relationship of Average latency of peer-to-peer and number of node

从图 7 可以看出，随着网络内节点数量的增多，平均端到端时延都在增大，其中 SDCM 的平均端到端时延最小。这是因为采用 SDCM 时网络内的传感器节点通过最短跳数的方式将数据包发送给数据收集节点，从而降低了数据拥塞的机会。

随着邻居节点密度的增加，Secs-TMP 方法在确定第一条数据发起节点时很容易造成网络拥塞，而 SDCM 通过随机挑选数据发起节点，因此具有较低的平均端到端时延。

6 结束语

针对目前基于移动 Sink 的 WSN 数据收集方法存在攻击检测率不高、内存开销大等问题，提出了一种基于移动 Sink 的 WSN 安全数据收集方法，利用改进的 ElGamal 方案实现消息认证，通过支持向量机对网络进行训练，确定剩余能量阈值，识别不同的网络攻击。仿真实验结果表明 SDCM 具有较高的攻击检测率、较低的内存开销。在后续的工作中，将研究 SDCM 方法在多媒体应用中的性能。

参考文献：

- [1] YICK J, MUKHERJEE B, GHOSAL D. Wireless sensor network survey[J]. Computer Networks, 2008, 52(12): 2292-2330.
- [2] MODIEGINYANE K M, MALEKIAN R, LETSWAMOTSE B B. Flexible network management and application service adaptability in software defined wireless sensor networks[J]. Journal of Ambient Intelligence and Humanized Computing, 2019, 10(4): 1621-1630.
- [3] RATIJIT M, SURAJ S. Proactive data routing using controlled mobility of a mobile Sink in wireless sensor networks[J]. Computers & Electrical Engineering, 2018, 70: 21-36.
- [4] BORAWAKE-SATAO R, PRASAD R S. Mobile Sink with mobile agents: effective mobility scheme for wireless sensor network[M]//Sensor Technology: Concepts, Methodologies, Tools, and Applications. 2020: 1035-1047.
- [5] YARINEZHAD R, SARABI A. Reducing delay and energy consumption in wireless sensor networks by making virtual grid infrastructure and using mobile Sink[J]. AEU - International Journal of Electronics and Communications, 2018, 84: 144-152.
- [6] JIAO X, LOU W, GUO S, et al. Delay efficient scheduling algorithms for data aggregation in multi-channel asynchronous duty-cycled WSN[J]. IEEE Transactions on Communications, 2019, 67(9): 6179-6192.
- [7] ZARZOOR A R, ABDULLAH M Z, SHILTAGH N A. Secure mobile sink node location in wireless sensor network using dynamic routing protocol[J]. Association of Arab Universities Journal of Engineering Sciences, 2019, 26(1): 113-120.
- [8] KAVIDHA V, ANANTHAKUMARAN S. Novel energy-efficient secure routing protocol for wireless sensor networks with mobile Sink[J]. Peer-to-Peer Networking and Applications, 2019, 12(4): 881-892.
- [9] FRANCESCO M D, SHAH K, KUMAR M, et al. An adaptive strategy for energy-efficient data collection in sparse wireless sen-

- sensor networks[C]//Wireless Sensor Networks, 7th European Conference, EWSN 2010. 2010: 17-19.
- [10] LAI S, RAVINDRAN B. An automatic presence service for low duty-cycled mobile sensor networks[J]. Mobile Networks & Applications, 2011, 16(4): 460-474.
- [11] TABIBI S, GHAFARI A. Energy-efficient routing mechanism for mobile sink in wireless sensor networks using particle swarm optimization algorithm[J]. Wireless Personal Communications, 2018, 104(1).
- [12] RESTUCCIAF, DAS S K. Optimizing the lifetime of sensor networks with uncontrollable mobile Sinks and QoS constraints[J]. ACM Transactions on Sensor Networks, 2016, 12(1): 1-31.
- [13] RASHEED A, MAHAPATRA R N. The three-tier security scheme in wireless sensor networks with mobile Sinks[J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 23(5): 958-965.
- [14] CONTI M, PIETRO R D, GABRIELLI A, et al. Secure topology maintenance and events collection in WSNs[J]. Security and communication networks, 2011, 4(7): 744-762.
- [15] RAJESWARI S R, SEENIVASAGAM V. Secured energy conserving slot-based topology maintenance protocol for wireless sensor networks[J]. Wireless Personal Communications, 2016, 87(2): 527-550.
- [16] RENOLD A P, CHANDRAKALA S. MRL-SCSO: multi-agent reinforcement learning-based self-configuration and self-optimization protocol for unattended wireless sensor networks[J]. Wireless Personal Communications, 2017, 96(4): 5061-5079.
- [17] NIKATE P M, MUJAWAR I I. Performance evaluation of floyd steinberg halftoning and jarvis haltonong algorithms in visual cryptography[J]. International Journal of Innovations in Engineering and Technology, 2015: 336-342.
- [18] CHANG Q, ZHANG Y, QIN L. A node authentication protocol based on ECC in WSN[C]//2010 International Conference on Computer Design and Applications. 2010.
- [19] MAIVIZHI R, YOGESH P. Secure in-network aggregation in wireless sensor networks[J]. International Journal of Intelligent Information Technologies (IJIIT), 2020, 16(1): 49-74.
- [20] HUANG S, CAI N, PACHECO P P, et al. Applications of support vector machine (SVM) learning in cancer genomics[J]. Cancer Genomics-Proteomics, 2018, 15(1): 41-51.
- [21] ERIKSSON J, ÖSTERLIND F, FINNE N, et al. Accurate network-scale power profiling for sensor network simulators[C]//European Conference on Wireless Sensor Networks. 2009: 312-326.
- [22] BOUGUERA T, DIOURIS J F, CHAILLOUT J J, et al. Energy consumption model for sensor nodes based on LoRa and LoRaWAN[J]. Sensors, 2018, 18(7): 2104.

[作者简介]



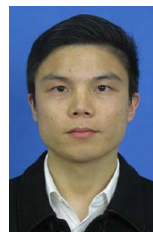
苗春雨（1978-），男，吉林四平人，博士，杭州安恒信息技术股份有限公司高级副总裁，主要研究方向为网络安全体系架构、传感网（物联网）安全。



范渊（1975-），男，浙江金华人，杭州安恒信息技术股份有限公司总裁，主要研究方向为应用安全、数据安全。



李晖（1969-），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码与信息安全、信息论与编码理论。



葛凯强（1992-），男，浙江绍兴人，杭州安恒信息技术股份有限公司工程师，主要研究方向为物联网安全。



张小孟（1983-），男，浙江温州人，杭州安恒信息技术股份有限公司高级副总裁，主要研究方向为应用安全、Web安全。