软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(Suppl.(1)):108−116

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于加权拟合分析的 WSN 安全数据融合机制研究*

李 平[1,2], 阳 武[1], 谢晋阳[1], 朱红松[2], 张永光[1], 李晓锋[3]

[1](长沙理工大学 计算机与通信工程学院,湖南 长沙 410114)

[2](中国科学院 信息工程研究所 信息安全国家重点实验室,北京 100093)

[3](北京控制工程研究所 软件研制中心,北京 100190)

通讯作者: 李平, E-mail: lping9188@163.com

摘 要: 传统的基于密码学方式的安全机制并不能有效解决妥协节点产生的假冒攻击问题,同时,基于簇头的信任判断和证实机制需要更多的通信开销,使得基于簇头的信任管理与认证是当前安全数据融合机制研究的焦点.以能量衰减模型的事件感知为研究场景,设计一种基于加权拟合分析的安全数据融合机制.在事件源情况未知的条件下,实现簇内节点对事件源距离的近似估计.研究具有簇属性特征的数据点基于所拟合曲线的分布性质,提出基于曲线簇分析的簇头信任判断机制.仿真实验结果表明,所提出的机制在曲线拟合精度、防妥协性能等方面有较高的提升,达到了预期的效果.

关键词: 数据融合;加权曲线拟合;无线传感器网络;安全

中文引用格式: 李平,阳武,谢晋阳,朱红松,张永光,李晓锋.基于加权拟合分析的 WSN 安全数据融合机制研究.软件学报,2013,24(Suppl.(1)):108−116. http://www.jos.org.cn/1000-9825/13012.htm

英文引用格式: Li P, Yang W, Xie JY, Zhu HS, Zhang YG, Li XF. Study on mechanisms of secure data aggregation based on weighted fitting analysis. Ruan Jian Xue Bao/Journal of Software, 2013,24(Suppl.(1)):108−116 (in Chinese). http://www.jos.org.cn/1000-9825/13012.htm

Study on Mechanisms of Secure Data Aggregation Based on Weighted Fitting Analysis

LI Ping[1,2], YANG Wu[1], XIE Jin-Yang[1], ZHU Hong-Song[2], ZHANG Yong-Guang[1], LI Xiao-Feng[3]

[1](School of Computer and Telecommunications, Changsha University of Science and Technology, Changsha 410114, China)

[2](State Key Laboratory of Information Security, Institute of Information Engineering, The Chinese Academy of Sciences, Beijing 100093, China)

[3](Software Development Center, Beijing Institute of Control Engineering, Beijing 100190, China)

Corresponding author: LI Ping, E-mail: lping9188@163.com

Abstract: Cryptographic approaches are vulnerable to impersonation attacks when nodes become compromised. Meanwhile, trust-based judgment and confirmation of cluster heads in WSN imposes higher communication cost. Trust management and authentication on cluster heads in WSN are essential in research on the mechanisms of secure data aggregation at present. In this paper, an energy attenuation model is adopted to describe event sensing in a kind of WSNs. Approximate evaluation on distance between occurring event and nodes within a cluster is achieved in case the location of the event is not known. Distribution properties of data points with clustering characteristics based on fitting curve construction are theoretically analyzed. In addition, the mechanism on trust authentication on cluster heads is also refined. Experimental results show that the proposed mechanism has much better performance on fitting accuracy and malicious CH recognition than previous works.

Key words: data aggregation; weighted fitting curve; WSN; security

* 基金项目: 国家高技术研究发展计划(863)(2013AA014002); 国家重点基础研究发展计划(973)(2011CB302902); 中国科学院信息工程研究所前瞻部署项目(Y3Z0071G02)

收稿时间: 2013-05-02; 定稿时间: 2013-08-22

数据融合技术是无线传感器网络(WSN)中进行数据处理获得准确查询结果且有效减少能耗的重要技术之一[1].由于 WSN 资源的限制,当传感器节点部署在敌方环境时,网络中的数据融合面临着严重的安全问题.攻击者可以俘获节点,同时修改或伪造传感节点的信息并重新部署到 WSN 中[2].由于节点被俘获而被攻击者利用形成的假冒攻击,不仅可以篡改自身的感知数据,如果是恶意簇头节点,还可以篡改簇内其他节点传输过来的数据.当前安全数据融合机制的研究大致可分为以数据为中心、基于剩余能量、最优化及基于性能的融合等几大类[3].但在数据融合准确性、融合效率与安全性能等因素的折中上值得深入研究.

基于"多数可信任"的信任模型是采用非密码学方式解决簇头节点假冒攻击的一般思路.基于能量衰减模型的事件数据具有较强的空间相关性.在事件源地点与能量值未知的前提下,如何将标识不同簇属性的数据点在拟合能量曲线的过程中有"区分性"地识别出来,是本文在安全数据领域中进行簇头信任判断研究的出发点.

1 相关工作

当前解决数据融合的安全问题主要可以分为两类,一类是基于密码学体系的安全数据融合,另一类是基于非密码学体系的安全数据融合.

SecureDAV[4]是 Mahimkar 等人提出的一个基于分簇型安全融合协议,ESPDA 是 Cam 等人提出的一种能量有效的安全数据融合协议[5].Du 等人提出了一种基于证人的数据融合安全方法[6],Przydatek 等人设计了一种大规模传感器网络的安全数据融合框架 SIA[7].

RSDA[8]是一种基于信誉的安全数据融合方案,其不仅有聚合功能而且还具有信誉评价机制,它结合对称密钥的地理位置信息来分发通信密钥.簇内每一节点都监听其邻居节点的行为,依据节点是否参与感应、传输、聚合等簇操作来计算节点信誉值,最后依据节点信誉值来选出簇头.

基于密码学方式的安全机制并不能有效解决妥协节点产生的假冒攻击问题,而基于信誉机制的安全数据融合对融合精度产生的影响较大.本文以能量衰减模型的事件感知为研究场景,提出一种基于加权拟合分析的安全数据融合机制.在事件源情况未知的条件下,提出簇内节点对事件源距离的近似估计算法,研究具有簇属性特征的数据点基于所拟合曲线的分布性质,提出基于曲线簇的簇头信任判断机制.

2 网络模型及攻击分析

本节给出假设的网络场景及攻击模型,为描述方便,给出了相关的术语与定义.

2.1 网络描述

对于一类基于能量衰减模型的事件监测型传感器网络中,事件源为一类地点与能量值未知的随机突发事件,传感器节点感知到的能量值期望满足能量衰减公式: $Z = A\mathrm{e}^{-\alpha d^{\theta}}, \theta > 0$. 其中,$A$ 表示事件源的能量(如温度等);d 是空间中该节点与事件源的距离(节点的事件距离);Z 是节点的能量观测值.θ,α为常数.根据上述公式,理论上所有节点的感知值及节点到事件源的距离在二维坐标上的映射(Z,d)都会落在能量衰减曲线上,然而,被篡改感知值的恶意节点将会偏离此曲线.

在 WSN 的有效感知范围内,假设能感知到有效能量值的节点集合为 V.文献[9]将所有节点动态分成 k 个簇,依次为 $V_1,V_2,...,V_k$,每个簇的节点数分别为 $|V_1|,|V_2|,...,|V_k|$, $V_i=\{a_1,a_2,...,a_{|V_i|}\mid i=1,2,...,k\}$ 表示 V_i 的所有节点的集合, $c_i(i=1,2,...,k)$ 为 V_i 的簇头节点.当发生事件后,簇 V_i 中的任意节点 a_s 将能量感知值 Za_s 、节点 ID 及其与邻居节点间的距离 $d_{si}(i=1,2,...,|V_i|)$ 等传到簇头节点 c_i . c_i 根据聚合函数[5]融合所有数据传输到 *Sink*,同时构造一个特征节点集合 V_{c_i} ,并将 V_{c_i} 的感知数据及节点之间的距离作为验证信息传输到 *Sink*.*Sink* 根据接收的特征节点集合中的数据进行距离估计、曲线簇拟合及恶意簇头节点的判断.

2.2 攻击模型

对于分簇的 WSN,在敌对的环境中通常存在两类攻击行为:一类是单独的恶意节点攻击,另一类是恶意簇攻击,本文的算法主要针对第 2 类攻击.对于恶意簇 V_i , c_i 篡改簇内某些节点的数据,使得 *Sink* 接收的所有数据中

包含一系列的虚假数据.若节点 a_u 是被 c_i 篡改的节点,假设 a_u 的感知值为 Za_u,那么 c_i 融合 a_u 的感知值 $Z'a_u$ 满足:

$$Z'a_u = Za_u + X_1, X_1 - N(\mu_1, \sigma_1^2), \text{and}, |Za_u - Z'a_u| > \zeta \tag{1}$$

2.3 术语与定义

定义 1(特征节点集合). 对于 V_i,假设感知值从小到大为 $Za_1, Za_2, ..., Za_{|V_i|}$ 的节点 $a_1, a_2, ..., a_{|V_i|}$,定义包含 $|V_{c_i}|$ 个节点的特征节点集合 $V_{c_i} = R\_V_{c_i} \cup S\_V_{c_i}$,其中 $S\_V_{c_i}$ 为 V_i 中任意选取的 $|S\_V_{c_i}|$ 个节点用于曲线拟合, $R\_V_{c_i}$ 为 $|R\_V_{c_i}|$ 个感知值最相近的节点用于节点距离估计,满足:

$$\eta_i = \sum |Z - \overline{Z}|^2 = \min\{\eta'\} = \min\left\{\sum |Z' - \overline{Z'}|^2\right\} \tag{2}$$

其中, η_i 为 $R\_V_{c_i}$ 中节点的相近程度系数, $\overline{Z}$ 为 $R\_V_{c_i}$ 中 $|R\_V_{c_i}|$ 个节点感知值的均值, $\overline{Z'}$ 为 V_i 中任意 $|R\_V_{c_i}|$ 个节点感知值的均值.

定义 2(特征圆). 假设事件源位于圆心,那么感知值相同的节点都会落在同一圆环上,定义所有感知值为 Z 的点组成的圆为特征圆$\odot Z$.

相关术语与约定见表 1.

Table 1 Terminology and conventions

表 1 相关术语与约定

符号	说明
O	事件源
c_i	簇 V_i 的簇头节点
η_i	$R\_V_{c_i}$ 节点的相近程度
$V_i, \|V\|$	所有节点集合,V 中的节点数量
V_i, V_{c_i}	第 i 个簇的节点集合, V_i 中特征节点的集合
$a, Za_i, Z'a_i$	节点的标识,节点 a_i 的感知值,节点 a_i 传输到 *Sink* 的感知值
$R\_V_{c_i}, S\_V_{c_i}$	V_i 中感知值相近的节点集合, V_i 中任意 $\|S\_V_{c_i}\|$ 节点集合,用于拟合
$d_{ij}, d''\|a\|, d\|a\|$	节点间的距离,节点 a 到事件源的距离估计,节点 a 到 O 的实际距离

定义 3(特征映像点). 假设事件源位于圆心 O,对任意的节点 $\{a_v \mid a_v \in R\_V_i\}$ 位于点 A,那么 OA 或其延长线与$\forall$特征圆$\odot Z$ 存在一个交点,定义此交点为 a_v 在特征圆$\odot Z$ 的特征映像点.

3 基于多簇加权拟合性质的判断机制

本节探讨构成恶意簇头判断机制的 3 个核心内容:

(1) 节点到事件源的距离(节点的事件距离)的理论估计及误差分析.事件距离估计的精确度直接影响到曲线拟合的精确程度及数据融合准确度,是簇头进行信任判断的重要影响因素;

(2) 加权曲线拟合.研究正常情况下来自多簇的数据点在拟合曲线上的分布特征,我们认为,正常节点与恶意簇头节点在曲线上的分布趋势应有所不同;

(3) 基于簇属性的恶意节点判断机制.

3.1 簇内节点的事件距离估计

假设 WSN 节点可通过 RSS,GPS 等方式得到其与邻居节点之间的物理距离[10],本节将详细分析簇内节点对的事件距离估计.

3.1.1 理论估计

如图 1 所示,对于同心圆上的 3 点 A,B,C 节点之间的距离 a,b,c,由几何关系易知:

$$r^2 = \frac{a^2b^2c^2}{2(a^2b^2 + a^2c^2 + b^2c^2) - a^4 - b^4 - c^4} \tag{3}$$

$$|OD|^2 = r^2 + e^2 - \frac{e(a^2+b^2-c^2)}{2b} + \frac{e(2r+a)(2r-a)(r-c)}{2r^2} \tag{4}$$

由式(3)、式(4)可知,若节点之间的距离 a,b,c,e 可知,则通过几何性质易知簇内任意节点到事件源的理论距离.

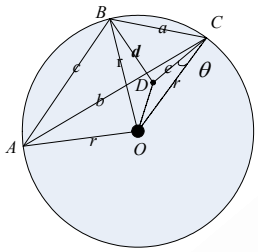


Fig.1 Geometric analysis of distance estimation

图 1 事件距离估计的几何分析

3.1.2 误差分析

(1) $R\_V_{c_i}$ 分析

由第 3.1.1 节可知,对于任意 V_i,节点到事件源的距离估计准确度依赖于 $R\_V_{c_i}$ 中节点感知值的相近程度 η.

性质 1. 对 V_i 中任意 $|R\_V_{c_i}|$ 个节点组成的集合构成 $|R\_V_{c_i}|$-组合集,表示为 $CV_i=\{CV_i^{(1)},CV_i^{(2)},...,CV_i^{(|CV_i|)}\}$,其中,$|CV_i|=C_{|R\_V_{c_i}|}^{|V_i|}$. $\forall CV_i^{(j)}\in CV_i(j=1,2,...,|CV_i|)$,令 $CV_i^{(j)}$ 中节点的感知值相近程度为 $\eta(CV_i^{(j)})$,则 $R\_V_{c_i}$ 中节点的感知值相近程度 $\eta(R\_V_{c_i})$ 满足 $\eta(R\_V_{c_i})=\min\{\eta(CV_i^{(1)}),\eta(CV_i^{(2)}),...,\eta(CV_i^{(|CV_i|)})\}$.

(2) 基于特征圆的距离误差分析

如图 2 所示,假设 (A,B,C) 是 $R\_V_{c_i}$ 中任意 3 个节点 a_u,a_v,a_w 的实际位置,$\overline{Z_i}$ 是 $R\_V_{c_i}$ 中所有节点的感知值均值,(A',B',C') 是 a_u,a_v,a_w 在 $\odot\overline{Z_i}$ 的特征映像点.由于 (A',B',C') 在同一特征圆上,则 $(|OA'|,|OB'|,|OC'|)$ 满足式(4).由于 $R\_V_{c_i}$ 的节点感知值不完全相等,且 $\angle ABA',\angle CAC',\angle BCB'$ 非常小,我们近似认为特征映像点之间的距离 (如$A'B',A'C',B'C'$) 满足:

$$\begin{cases} |A'B'|=|AB|-|AA'|-|BB'|,|OA|=|OA'|+|AA'| \\ |B'C'|=|BC|-|BB'|+|CC'|,|OB|=|OB'|+|BB'| \\ |A'C'|=|AC|-|AA'|+|CC'|,|OC|=|OC'|-|CC'| \end{cases} \tag{5}$$

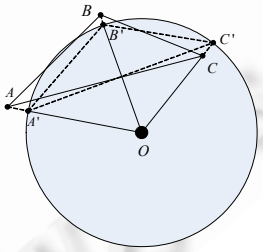


Fig.2 Analysis on distance and error estimation

图 2 含有误差分析的距离估计

由于 $\overline{d}=|OA'|=|OB'|=|OC'|$.结合能量衰减公式、式(4)、式(5)、式(7)、式(8),则节点到事件源的估计距离满足 $d'|a_u|=\overline{d}+|AA'|$.

(3) 估计距离的二项式处理

由第 3.1.1 节可知,对于簇 V_i 的特征节点集合 V_{c_i},$R\_V_{c_i}$ 中每 3 个不同的节点便能得到所有特征节点到事件

源的一组距离.因此,对于所有 V_{c_i} 中每个特征节点存在 $C^3_{|R\_V_{c_i}|}$ 组距离估计,我们对每个节点的所有 $C^3_{|R\_V_{c_i}|}$ 个距离估计值做均值处理后得到节点到事件源的最终距离估计值如下:

$$d''|a_u|=\frac{\sum_{i=1}^{p} d_i|a_u|}{p},\ u=1,2,...,|V_{c_i}|,\ p=C^3_{|R\_V_{c_i}|} \tag{6}$$

3.2 簇间加权拟合性质

定义 4(拟合簇序列). 连续 $t(1\leqslant t\ll k)$ 个簇组成的集合 $\{V_j,V_{j+1},...,V_T \mid j=1,2,...,T,T=j+t-1\leqslant k\}$ 称为拟合簇序列,表示为 V_{jF} ,相应的补集称为互补拟合簇序列,表示为 $C_V(V_{jF})$.

定义 5(曲线族 $C_{(T)}$). 依次将 $V_{jF}(j=1,2,...,T,T=k-t+1)$ 拟合成能量衰减曲线 $C_1,C_2,...,C_T$,定义由上述曲线构成的集合为曲线族 $C_{(T)}$.

定义 6(归属曲线). 对于任意一个节点 $a_u\in V_i(i=1,2,...,k)$,若 a_u 参与任意一条曲线,如 C_j 的拟合,则称 C_j 为 a_u 的归属曲线,否则,称 C_j 为 a_u 的非归属曲线.

对于 V_i ,节点的事件距离估计精确度依赖于 $R\_V_{c_i}$ 中节点感知值的相近程度 η_i .本文将 η_i 作为最小二乘曲线拟合的一个权值,减少曲线拟合的误差,此时节点的感知值和估计距离满足式(7),当 σ 取最小值时为最优解.

$$\sigma=\sum_{i=1}^{t}\sum_{j=1}^{|V_{c_i}|}\eta_i(Z_{ij}-A\mathrm{e}^{-\alpha d^{\theta}})^2 \tag{7}$$

式中 Z_{ij} 为第 i 个簇中参与拟合的第 j 个节点的感知值.

定义 7(节点的映射). 设任意节点 a_u 对应于坐标上的数据点为 $(d''|a_u|,Za_u)$. 对于曲线族上任意一条曲线,如 $C_j\in C_{(T)}$,该曲线上能量值为 Za_u 的一点称为节点 a_u 在曲线 C_j 上的映射点,记作 $(d''_j|a_u|,Za_u)$.

由第 3.1 节的距离估计模型,假设对任意 a_u 的估计距离服从 $X_2-N(\mu_2,\sigma_2^2)$,其中, $\mu_2=d|a_u|$.

性质 2. 若感知值为 Za_u 的节点 a_u 非归属曲线 C_j ,节点 a_u 的估计距离 $d''|a_u|$ 与节点 a_u 在曲线 C_j 上的映射距离 $d''_j|a_u|$ 满足概率公式:

$$\lim_{\beta\to\infty}P\{|(d''_j|a_u|-d''|a_u|)|<\beta\sigma\}=1 \tag{8}$$

证明:由任意 a_u 的距离估计服从 $X_2-N(\mu_2,\sigma_2^2)$,那么节点 a_u 的实际估计距离 $d''|a_u|$ 在 $[\mu-\beta\sigma,\mu+\beta\sigma]$ 的概率为 $P=\int_{\mu-\beta\sigma}^{\mu+\beta\sigma}\frac{\mathrm{e}^{-\frac{(x-\mu)^2}{2\delta^2}}}{\sqrt{2\pi}\delta}\mathrm{d}x$, 而 $\lim_{\beta\to\infty}P=1$. □

由性质 2 可知,若 a_u 非归属曲线 C_j ,且 V_i 中超过 m 个特征节点同时对超过 t 条非归属曲线都满足式(9),那么我们认为簇 V_i 可能是恶意簇.

$$|(d''_j|a_u|-d''|a_u|)|>\varepsilon(\varepsilon>\beta\sigma) \tag{9}$$

如图 3 所示,假设 $C_{(T)}$ 均匀地分布在理想的能量衰减曲线的两边,从上到下依次标记为 $C_1,C_2,...,C_T$, V_{c_i} 中对应于坐标上的数据点在曲线 $C_j(j=1,2,...,T)$ 上边和下边的数量分别为随机变量 $Y_{上}(ij)$ 和 $Y_{下}(ij)$.

性质 3. 对 V_{c_i} 的所有节点对应于坐标上的数据点在 $C_j(j=1,2,...,T)$ 上边的数量的随机变量 $Y_{上}(i1),Y_{上}(i2),...,Y_{上}(iT)$ 满足: $E[Y_{上}(i1)]+...+E[Y_{上}(iT)]\approx(|V_{c_i}|\times T)/2$.

证明:由于任意 a_u 的距离估计服从 $X-N(\mu,\sigma^2)$, 当 $(d''|a_u|,Za_u)$ 落在理想曲线上方时满足 $d|a_u|-d''|a_u|>0$,由正态分布的性质易知 $P\{d|a_u|-d''|a_u|>0\}=0.5$,那么 V_{c_i} 中对应于坐标的数据点落在理想曲线上方个数的期望为 $|V_{c_i}|$.同理,由于 $C_1,C_2,...,C_T$ 均匀地分布在理想的能量衰减曲线的两边,那么有:

$$E[Y_{上}(i1)]+E[Y_{上}(iT)]\approx|V_{c_i}|,E[Y_{上}(i2)]+E[Y_{上}(i(T-1))]\approx|V_{c_i}|,...,E\left[Y_{上}\left(i\frac{T}{2}\right)\right]+E\left[Y_{上}\left(i\left(\frac{T}{2}+1\right)\right)\right]\approx|V_{c_i}| \tag{10}$$

所以, $E[Y_{上}(i1)]+...+E[Y_{上}(iT)]\approx(|V_{c_i}|\times T)/2$. □

根据性质 3,对于 V_i,依次统计 V_{c_i} 中对应坐标的数据点落在 $C_1,C_2,...,C_T$ 上方个数分别为 $y_{\perp}(i1),y_{\perp}(i2),...,y_{\perp}(iT)$,当 $|y_{\perp}(i1)+y_{\perp}(i2)+...+y_{\perp}(iT)-(l_i\times T)/2|\geqslant\lambda$ 时,我们认为簇 V_i 可能是恶意簇.

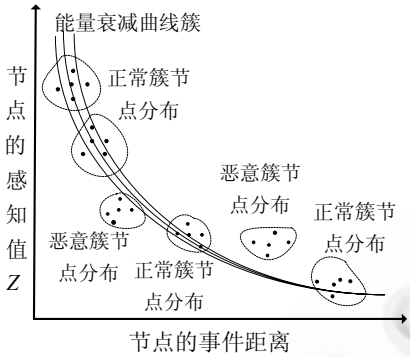


Fig.3 Energy attenuation formula based on judgment of malicious cluster diagram

图 3 基于能量衰减曲线的恶意簇判断图示

4 实验与仿真

为了验证本文提出的安全数据融合算法的性能,本文算法与基于信誉机制的 RSDA 进行了对比仿真实验.在 100m×100m 的区域内随机生成 1 024 个节点,事件源位于 (0,0) 处,并根据文献[4]中的方法动态生成 40 个簇.依次对每个簇中添加 1,2,...,10 个随机篡改感知值的恶意节点.对于上述场景,反复运行 1 000 次,分别进行模拟恶意节点的比例以及 R_V_i 中节点的相近程度 η_i 等对簇内节点的事件距离估计准确率、融合精度等关于算法性能指标的实验.

4.1 节点事件距离估计及融合精度

根据本文提出的算法,首先对节点的事件距离估计的准确性进行仿真测试,对于 V_i,由第 3.1 节,节点事件距离的估计依赖于 R_V_i 中节点的相近程度 η,以及恶意簇头篡改簇内节点感知数据的数量,本实验设定恶意簇篡改恶意节点的比例为 0~25%,η 的取值为 0~8,测试节点事件距离估计的误差以及数据融合精度.

由图 4 所示的三维图可知,随着网内恶意节点的增加,节点的事件距离估计误差明显增加,但绝大部分在 15%以内,因为尽管恶意节点的比例有所增加,但是节点事件距离的估计准确率主要受 η 的影响,个别误差超过 15%的原因是节点的相近程度系数偏高,以及节点的测试距离的误差较大.而随着 η 的增加,节点的事件距离估计准确率并没有明显下降是因为网内布置的节点密度较高,导致簇内 R_V_i 节点集合的相近程度整体都比较高,尽管 η 在增加,但是增加的幅度并不明显,所以对节点的事件距离估计的影响并不是太大.整体误差依然保持在 20%以内.

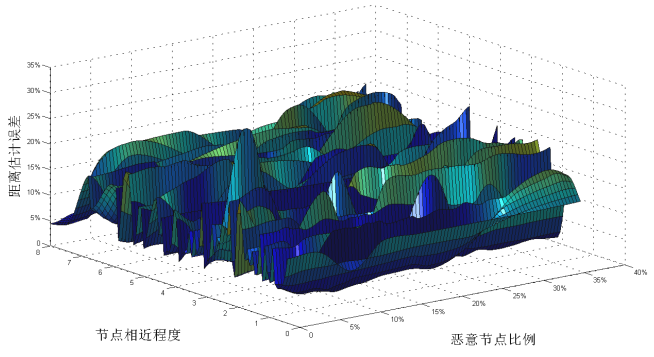


Fig.4 Event distance estimation accuracy

图 4 事件距离估计准确率

如图 5 所示,随着恶意节点比例的增加,本文提出的算法的数据融合精度明显比 RSDA 算法要高,因为基于信誉机制的恶意节点识别方式对“可信实体”有较高的要求,随着网内恶意节点比例的增加,网络的不可信程度增加,该机制识别恶意节点的能力明显下降.而本文提出的算法只要求一部分特征节点的信誉度高就可以提高融合精度.由于节点的密集度较高,同时本算法对节点数据融合前剔除了一些恶意簇数据,所以融合精度会比基于信誉度的识别机制明显提高.根据能力衰减公式,同样地,曲线拟合的精确度也依赖于节点事件距离估计的准确性.

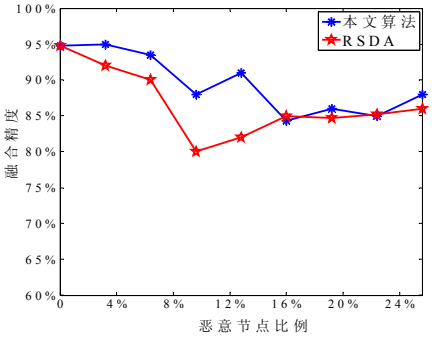


Fig.5 Fusion accuracy

图 5 融合精度

4.2 曲线拟合精度

由于本文提出的识别恶意节点恶意簇的算法的精度主要受曲线拟合精度的影响,本节通过实验分析曲线簇中参与拟合的簇的数量以及拟合时网络中恶意节点的数量对曲线拟合精度的影响.

由图 6 可知,随着参与曲线拟合的簇数量的增加,拟合的精度并没有理想地增加,根据式(7),随着 t 的增加,σ 的取值会越来越小,但是此时恶意簇对拟合的影响越来越大,而且这一影响并非呈线性增长,所以出现了随着 t 的增大并没有增加的情况.由图 7 可知,随着恶意节点比例的增加,拟合精度明显下降,同时曲线拟合精度并没有随着恶意节点比例的增加出现非线性的下降是因为曲线拟合受到簇内特征节点本身存在的测量误差以及最小二乘估计本身存在的偶然误差的影响,此时,在恶意节点比例偏小的情况下,并不会对拟合精度有过大的影响.

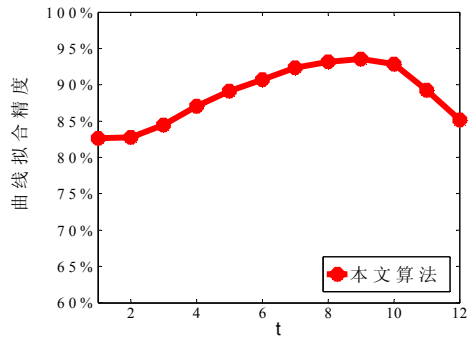


Fig.6 t – The accuracy of curve fitting

图 6 t——曲线拟合精度

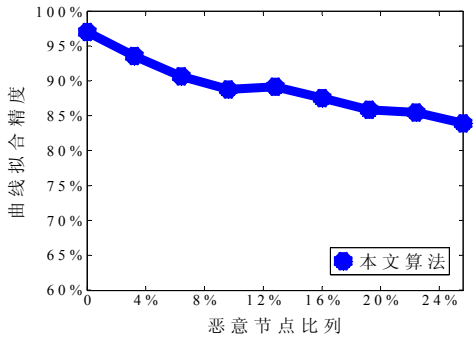


Fig.7 The proportion of malicious nodes-Curve fitting

图 7 恶意节点比例对曲线拟合精度的影响

4.3 恶意节点恶意簇的识别仿真

由第 4.1 节可知,节点的事件距离估计受 R_V_i 中 η 的影响并不大,同时,在恶意节点比例偏小时对其影响也比较小,然而根据能量衰减公式,节点事件距离估计对曲线拟合以及曲线簇的形成会起到决定性的作用,由图 4 及性质 3 可知,本文的算法对恶意簇头节点的识别依赖于曲线簇分布的精确程度,然而根据式(7),曲线簇的精确

程度依赖于 t 以及恶意簇的数量.假设我们拥有比较精确的曲线簇,对于单个恶意节点的判断根据性质 2,单个恶意节点的判断依赖于节点的估计值偏离其在曲线上的映射程度即系数 β,根据性质 3 和式(10),恶意簇头节点的判断依赖于簇内节点在曲线簇上下的偏离程度以及节点在曲线簇上下的分布比例,基于此,本节主要讨论本算法随着恶意节点比例的增加对恶意节点恶意簇头节点的识别性能上的影响.具体结果如图 8~图 10 所示.

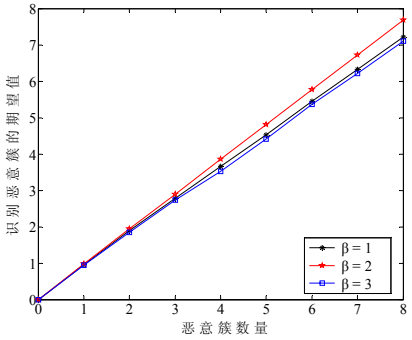


Fig.8 β – The expectation of identify malicious clusters

图 8 β——识别恶意簇的期望

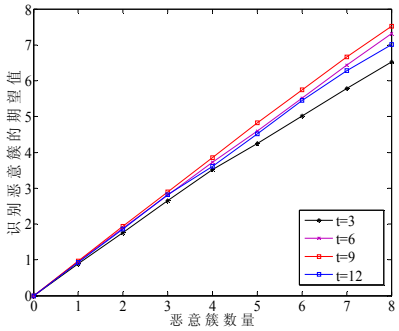


Fig.9 t—The expectation of identify malicious clusters

图 9 t——识别恶意簇的期望

根据本次模拟实验中节点布置的特点以及本算法的特点,本实验依次设定 $\beta=1,2,3$, $t=3,6,9,12$, λ=3,6,9.随着网络中恶意簇比例的增加,仿真本算法对恶意簇的识别性能.图 8 表示β不同取值时,随着恶意簇的增加本文算法对恶意簇识别的性能,尽管随着网络中恶意节点比例的增加,本算法对恶意簇识别的比例在下降,但当 $\beta=2$ 时情况较为理想,依然识别比例在 90% 以上.图 9 表示 t 的不同取值时,随着恶意簇的增加,本文算法对恶意簇识别的性能,当 $t=9$ 时,本文的算法对网络中恶意簇的识别效果明显好于其他取值时,这是因为,如果 t 太小,参与曲线拟合的簇偏少,影响了曲线拟合的精确度.然而当 t 偏大时,由于参与拟合的簇偏多,导致曲线簇中曲线数量偏少,由于节点事件距离测量时的偶然误差影响了本算法的性能.如图 10 所示,表示λ不同取值时,随着恶意簇的增加,本文算法对恶意簇识别的性能.由性质 3 可知,如果λ偏小,可能会使非恶意簇被认为是恶意簇;如果λ偏大,可能会使一些恶意簇被认为是正常的簇.如图 11 所示,通过给定不同的λ取值,对性能产生不同的影响,当 λ=6 时情况较为理想.

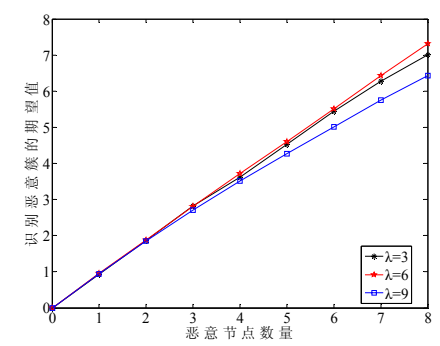


Fig.10 λ – The expectation of identify malicious clusters

图 10 λ——识别恶意簇的期望

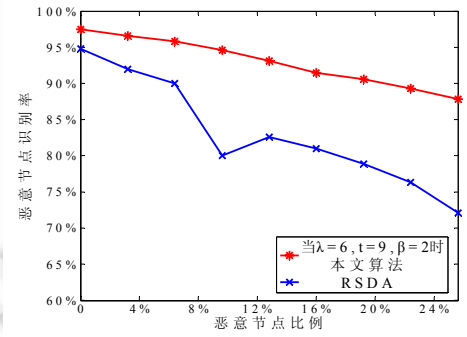


Fig.11 The rate of malicious node identification

图 11 恶意节点识别率

通过上面分析可知,一些关键变量对本算法的性能影响较大,本文通过选择上面实验得出的比较理想的变量取值,与 RSDA 的性能进行对比.如图 11 所示,当 $\beta=2$, $t=9$, $\lambda=6$ 时,本算法对恶意簇、恶意节点的识别性能明显比 RSDA 要高.

5 结束语

本文以能量衰减模型的事件感知为研究场景,提出一种基于加权拟合分析的安全数据融合机制.在事件源情况未知的条件下,提出簇内节点对事件源距离的近似估计算法,实验结果表明,此算法对节点的事件距离估计准确率较高.同时,本文研究具有簇属性特征的数据点基于所拟合曲线的分布性质,提出基于曲线簇的簇头信任判断机制.仿真实验表明,所提出的机制在曲线拟合精度、防妥协性能等方面有较高的提升,达到了预期的效果.

References:

[1] Ozdemir S, Xiao Y. Secure data aggregation in wireless sensor networks: A comprehensive overview. IEEE Trans. on Computer Networks, 2009,53:2022−2037.

[2] Intanagonwiwat C, Govindan R, Estrin D. Directed diffusion: A scalable and robust communication paradigm for sensor networks. ACM SIGPLAN Notices, 2000, 56−67.

[3] Zhao J, Govindan R, Estrin D. Computing aggregates for monitoring wireless sensor networks. Sensor Network Protocols and Applications, 2003, 139−148.

[4] Mahimkar A, Rappaport TS. Secure DAV: A secure data aggregation and verification protocol for wireless sensor networks. In: Proc. of the 47 th IEEE Global Telecommunications Conf. (Globecom). Dallas, 2004.

[5] Cam H, Ozdemir S, Muth D. ESPDA: Energy efficient and secure pattern-based data aggregation for wireless sensor networks. IEEE Computer Communications 29, 2006. 446−455.

[6] Du W, Deng J, Han YS, Varshney PK. A witness-based approach for data fusion assurance in wireless sensor networks. IEEE GLOBECOM, 2003, 1435−1439.

[7] Przydatek B, Song D, Perrig A. Secure information aggregation in sensor networks. In: Proc. of the SenSys 2003. ACM, 2003. 255−265.

[8] Alzaid H, Foo E. RSDA: Reputation-Based secure data aggregation in wireless sensor networks. In: Proc. of the 1st Int'l Workshop on Sensor Networks and Ambient Intelligence. Dunedin Academic Press, 2008. 36−42.

[9] Ayughi F, Faez K, Eskandari Z. A non location aware version of modified LEACH algorithm based on residual energy and number of neighbors. In: Proc. of the Conf. on Advanced Communication Technology. Phoenix Park, 2010. 1076−1080.

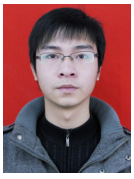
[10] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Communication Magazine, 2002,27(40): 102−114.

李平(1972－),男,湖南新化人,博士,教授,CCF 会员,主要研究领域为物联网,信息安全,数据挖掘.
E-mail: lping9188@163.com

朱红松(1973－),男,博士,副研究员,CCF 高级会员,主要研究领域为无线通信,无线传感器网络,虚拟技术,物联网大数据安全分析与智能处理.
E-mail: zhuhongsong@iie.ac.cn

阳武(1990－),男,硕士,主要研究领域为信息安全,物联网,数据挖掘.
E-mail: 1013568049@qq.com

张永光(1990－),男,硕士,主要研究领域为信息安全.
E-mail: 289345459@qq.com



谢晋阳(1989－),男,硕士,主要研究领域为信息安全,物联网,数据挖掘.
E-mail: 505354246@qq.com

李晓锋(1982－),男,学士,主要研究领域为嵌入式软件开发.
E-mail: 13501127502@126.com