文章编号:1671 - 6833(2019)01 - 0038 - 06

基于时序信息分析的 WSN 贝叶斯信誉评价模型

滕志军[1], 郭力文[1], 吕金玲[1], 侯艳权[2]

(1.东北电力大学 信息工程学院,吉林 吉林 132012; 2.国网七台河供电公司,黑龙江 七台河 154600)

摘 要: 为了有效降低信道占用对节点信誉评价的影响,提高信誉评价模型的准确性,针对数据中断攻击和选择性转发攻击,结合信道状态对网络的影响,引入节点行为时间序列和信道状态时间序列,提出了基于时序信息分析的 TS-BRS 信誉模型.采用时序分析法,对两条时间序列匹配分析,降低信道冲突对信誉评价模型的干扰,提高模型识别的准确性;并在信誉值更新中引入适应性维护函数 μ,加重现阶段节点行为对信誉值的影响,提高评价模型的适应性.仿真实验表明,新的信誉评价模型能有效提升模型的检测率和检测速度.引入维护函数,网络中被捕获的恶意节点的信誉值可以更快收敛.

关键词: 无线传感器网络; 时间序列; 贝叶斯理论; 信誉评价; 信道

中图分类号: TN92 **文献标志码**: A **doi**:10.13705/j.issn.1671 - 6833.2019.01.007

0 引言

无线传感器网络已经在越来越多的领域应用,如环境监测、森林防火、智能家居、工业生产、军事监测、医疗领域等[1].但网络节点部署环境的复杂性、节点间灵活自组和拓扑结构变化等,也导致其易遭受攻击,破坏网络的正常运行[2].无线传感器网络的内部攻击主要由恶意节点引起,因此检测与排除恶意节点也成为传感器网络安全的研究重点.针对内部攻击,搭建信誉模型是非常有效的方法.典型的贝叶斯信誉模型将节点的信任度进行量化并建立相应的信任管理机制,可有效提高网络安全性[3].

Ganeriwal 等[4]提出经典的贝叶斯信誉评价模型 BRSN 并应用于无线传感器网络,该模型将贝叶斯公式与 Beta 分布进行拟合,通过对 Beta 分布计算其期望值从而得到节点的信誉值.盛燕[5]提出了 NRRS 信誉评价模型,该算法在直接信誉与间接信誉上加入了路径管理,改进了邻居监测机制.杨光等[6]提出 MA&TP-BRSN 评价模型,通过引入节点行为评价,为监测节点状态奠定了基础,改进评价模型消除了评价的单一性,也让第三方节点评价更加客观.陈志奎等[7]提出基于信任云的传感器网络评估模型,将节点近期行为通过历史信任云和近期信任云分配权重,同时利用相似度对权重进行修正.Ouyang 等[8-9]提出 RD-HBRS 信誉评价模型,利用联合信息熵对第三方参考信息进行去冗余,降低网络能耗,利用高斯径向基函数识别亚攻击节点.崔慧等[10]在 WTE 基础上提出数据包技术策略,利用 MNDSDF 算法检测恶意节点,使得算法适应度更高.韩挺等[11]提出面向 MANET 的多属性路由评价 MDF-Trust,通过整合网络中的四项属性并分配相应权重来决策网络安全,有效地反映路由节点状态变化.

上述文献建立的信誉模型为该领域的研究提供了扎实的理论基础,但针对传感器网络中信道占用问题,只是通过控制环境参数或分配权重,效果并不理想.笔者针对无线传感器网络中信道拥堵所造成的误检,通过引入时间序列达到检测数据包传递状态和目标节点行为及状态,搭建基于时序信息分析的 TS-BRS(time-series WSN hierarchical beta reputation system)模型判定节点行为;同时引入维护函数维护通信统计量,完善信誉值模型,使得被捕获节点可以快速降低其信誉值,降低恶意节点对网络产生的负面影响.

收稿日期:2018 - 09 - 05;**修订日期**:2018 - 11 - 02

基金项目:国家自然科学基金资助项目(51277023);吉林省教育厅“十三五”科学研究规划项目(JJKH20180439KJ)

作者简介:滕志军(1973—),男,吉林吉林人,东北电力大学教授,博士,主要从事无线通信技术研究,E-mail:tengzhijun@163.com.

1　信誉模型建立

TS-BRS 模型依托于成簇式分层网络拓扑结构,网络结构分为汇聚节点(SINK)、簇头节点、普通节点. 簇内节点间可进行多跳通信,如图 1 所示. 节点信誉值计算采用时序分析法,底层普通节点负责采集目标节点在阶段时间内信道状态信息和节点行为信息,生成相应的时间序列并交由簇头统一匹配运算[12]. 簇头节点通过融合簇内各节点时间序列,分析目标节点行为,计算目标节点阶段时间内正常行为和非正常行为,其中非正常行为分恶意行为与非恶意行为,然后通过贝叶斯公式计算各节点信誉值. 节点信誉值管理采用层次化管理模式,信誉值由簇头存储. 汇聚节点可以对全局信誉进行查询,跨簇信誉值查询也需要汇聚节点协调完成.

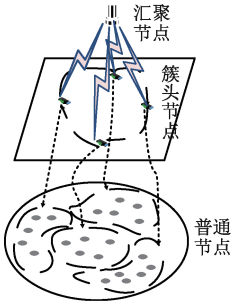

图 1　网络结构

Fig. 1　Network structure

由于无线传感器网络允许丢失路由信息,所以只对网络中数据包的传递进行监测,示例路径如图 2 所示. 数据包由节点 N_1 经过节点 N_2 传递到节点 N_3,节点 N_4、N_6 为节点 N_2 的邻居侦听节点,节点 N_5 为节点 N_3 的邻居侦听,A 和 B 为簇内其他节点的集合,$A=\{N_k \mid k\neq 1,2,3,4\}$,$B=\{N_k \mid k\neq 1,2,3,5\}$,其中 $A\cap B\neq 0$.

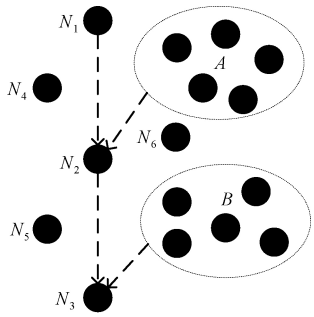

图 2　示例路径

Fig. 2　Example path

1.1　贝叶斯信誉评价模型

信誉评价采用贝叶斯信誉模型. 通常对一个目标信誉度的评价取决于该目标历史行为记录. 而信誉度亦可以对目标未来行为进行预测[13]. 通过数学运算与收集数据的拟合,贝叶斯理论可以描述信誉值的变化规律,利用先验概率事件,更新最近的相关证据,然后对未来行为进行预测. 利用贝叶斯信誉分布与 Beta 分布进行拟合,联系示例节点 N_2 信誉评价(见图 2),节点 N_2 的信誉评价函数如下:

$$D_{N_2}=E(f(\alpha_{N_2},\beta_{N_2}))=\frac{\alpha_{N_2}}{\alpha_{N_2}+\beta_{N_2}},\quad (1)$$

式中:D_{N_2} 为节点 N_2 的信誉值;α_{N_2} 和 β_{N_2} 分别表示正负级评分,在这里表示节点 N_2 正常通信和恶意通信的次数,其中:

$$f(p;\alpha_{N_1},\beta_{N_2})=\frac{\Gamma(\alpha_{N_2}+\beta_{N_2})}{\Gamma(\alpha_{N_2})\Gamma(\beta_{N_2})}p^{\alpha-1}(1-p)^{\beta-1},\quad (2)$$

表示节点正常通信的概率密度函数,p 表示节点正常通信的概率.

1.2　时间序列建立与分析

1.2.1　通信行为时间序列

判断节点 N_2 通信行为采用 *ACK* 两跳回传机制和邻居看门狗机制. 当节点 N_1 经由节点 N_2 把信息传递给节点 N_3,节点 N_1 会先将数据包保存一段时间,节点 N_2 与节点 N_3 收到数据包会给节点 N_1 发送简单的回执信息. 当节点 N_1 收到节点 N_3 的回执信息,则认定数据包传输成功,回执信息由报文头部、源节点地址、转发节点地址、目的节点地址和签名信息构成.

节点 N_1 记录数据包传输成功的次数 n 和生成数据包传输失败的时间序列 $\boldsymbol{TCI}_{N_2}$,即没有收到节点 N_3 的回执信息的时间序列. 示例序列如下所示:

$$\boldsymbol{TCI}_{N_2}=\begin{bmatrix} t_1 & t_3 & t_4 & t_5 & t_6 & t_7 \\ N_1 & N_1 & N_1 & N_1 & N_1 & N_1 \end{bmatrix},\quad (3)$$

式中:第一行为 Δt 内的时间序列;第二行为发送数据包的源节点.

相同方式生成集合 A 内节点记录的通信行为序列 $\boldsymbol{TCA}_{N_2}$,示例序列如下所示:

$$\boldsymbol{TCA}_{N_2}=\begin{bmatrix} t_2 \\ A \end{bmatrix}.\quad (4)$$

1.2.2　信道状态及行为时间序列

在图 2 的网络成簇后,节点 N_1 通信半径 R 内的节点为节点 N_1 下一跳的侦听节点,示例节点 N_4 为侦听节点. 侦听节点负责侦听目标节点在 Δt 内信道状态和行为并生成信道状态时间序列 $\boldsymbol{TS4}_{N_2}$,示例序列为:

$$\boldsymbol{TS}4_{N_2}=\begin{bmatrix} t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 \\ A & 0 & 0 & N_1 & N_1 & N_1 & N_1 \\ * & * & * & 1 & 1 & 0 & 1 \end{bmatrix}, \quad (5)$$

式中:第一行为 Δt 内的时间序列,第二行为目标节点 N_2 在 t_i 时刻信道状况. 每个节点有一个侦听邻居表,当 N_1 广播搜索目标节点 N_2,N_1 广播半径内的侦听节点查找各自侦听邻居表内是否有目标节点 N_2,如有则开始侦听. 从侦听节点 N_1、N_2 间的四次握手和两次回执,到确认第二次回执做一次信道记录,空闲时刻不做记录. 文中为了说明方便,空闲时刻记 0. 示例序列 $\boldsymbol{TS}4_{N_2}$ 在 t_1 时刻表示节点 N_2 的信道被集合 A 内的节点占用,t_2、t_3 时刻节点 N_4 没有侦听到节点 N_2 有通信行为,t_4、t_5、t_6、t_7 时刻节点 N_2 信道被节点 N_1 占用. 第三行为节点 N_2 收到数据包后的转发行为,若节点 N_4 侦听到节点 N_1 数据包目的地址为 N_2,不做记录. 当目的地址不为 N_2,则需要侦听节点 N_2 的转发行为,有转发行为记为 1,没有转发行为记 0. 因为空闲时刻记 0,以及示例路径为 $N_1\rightarrow N_2\rightarrow N_3$,故暂记 $t_1t_2t_3$ 时刻转发行为记为 *(空),以方便讨论.

同样生成节点 N_2 由侦听节点 N_6 侦听所生成的时间序列 $\boldsymbol{TS}6_{N_2}$(见式 6). 为简述方便,不在示例路径内转发行为都记为 *. 经过 Δt 各个侦听节点将侦听的时间序列发送给簇头,簇头将各节点的时间序列进行时序匹配融合. 如图 2,将示例路径中的所得的两条时间序列进行时序匹配融合,生成时间序列 TS_{N_2}(见式 7).

$$\boldsymbol{TS}6_{N_2}=\begin{bmatrix} t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 \\ A & A & 0 & 0 & 0 & N_1 & N_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{bmatrix}. \quad (6)$$

$$\boldsymbol{TS}_{N_2}=\begin{bmatrix} t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 \\ A & A & 0 & N_1 & N_1 & N_1 & N_1 \\ * & * & * & 1 & 1 & 0 & 1 \end{bmatrix}. \quad (7)$$

相同方法生成节点 N_3 的融合状态时间序列 $\boldsymbol{TS}_{N_3}$(见式 8),同样为简述方便,不在示例路径内的信道状态和转发行为都记为 *. 因为数据包由节点 N_2 传输给节点 N_3 所产生的时间序列会有一定时延 ε,所以在时序匹配时,节点 N_3 的状态时间序列允许一定时间误差,其中 $0<\varepsilon<\nu$,ν 为所允许的最大时间误差.

$$\boldsymbol{TS}_{N_3}=\begin{bmatrix} t_1+\varepsilon t_2+\varepsilon t_3+\varepsilon t_4+\varepsilon t_5+\varepsilon t_6+\varepsilon t_7+\varepsilon \\ * \quad * \quad * \quad B \quad N_2 \quad 0 \quad 0 \\ \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \end{bmatrix}. \quad (8)$$

1.2.3 时间序列匹配与分析

经过 Δt,普通节点将各自记录的通信行为序列和状态行为序列统一发送到簇头节点,簇头先将各节点序列融合,示例路径中节点 N_2 的通信行为时间序列为 $\boldsymbol{TCI}_{N_2}$ 和 $\boldsymbol{TCA}_{N_2}$ 的并集,记为 $\boldsymbol{TC}_{N_2}$:

$$\boldsymbol{TC}_{N_2}=\begin{bmatrix} t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 \\ N_1 & A & N_1 & N_1 & N_1 & N_1 & N_1 \end{bmatrix}. \quad (9)$$

结合式(7)~(9)和示例路径 $N_1\rightarrow N_2\rightarrow N_3$ 信息传输失败的所有状况,通过时序分析法,可知节点 N_2 在各时刻的详细状态. t_1 时刻显示节点 N_2 与集合 A 内的节点进行通信行为,由于节点信道被占用,故不记为节点 N_2 通信失败;t_2 时刻显示数据包传输源节点为集合 A 内的节点,不在示例路径中,故先不做统计;t_3 时刻显示源节点 N_1 无法与节点 N_2 进行通信行为,侦听节点也没侦听到节点 N_2 有其他通信行为,数据产生中断,故记为节点 N_2 通信失败;t_4 时刻显示节点 N_2 有正常的转发行为,节点 N_3 信道与集合 B 内的节点进行通信行为,子节点信道被占用,故不记为节点 N_2 通信失败;t_5 时刻显示节点 N_2 有正常的转发行为,节点 N_3 无通信行为,且没有正常回复回执信息,故不记为节点 N_2 通信失败,节点 N_3 将由节点 N_2 记录通信失败;t_6 时刻显示节点 N_2 没有正常转发行为,故记为节点 N_2 通信失败;t_7 时刻显示节点 N_2 无法与节点 N_3 进行通信行为,且节点 N_2 由正常转发行为,故不记为节点 N_2 通信失败,节点 N_2 将对节点 N_3 记录通信失败.

1.3 信誉值更新及统计

传感器网络信息传输失败的原因有很多,环境干扰、信道冲突等都会对数据包传输造成影响,故将所有的信息传输失败皆视为恶意节点所造成的影响,会导致节点信誉值较低. 而经由时序分析的侦听过程可以检测出信道占用所造成的干扰,提高侦听检测的准确性.

节点的信誉值基于节点的历史行为,可分为正常通信行为、恶意节点行为和信道占用行为,信道占用行为不进入信誉值评价标准. 当通信次数越多,现阶段行为的影响力越小. 通过引入维护函数 μ,见式(10),将节点历史信誉值近似约分,降低历史总通信次数,增加现阶段行为的影响力,改变节点信誉值的弹性. 预设定的维护值 θ 的影响由仿真图 7 所示,具体取值按环境、网络表现等因素,将在未来的研究中做深入的讨论研究. 联系示例节点 N_2,节点信誉值为 D_{N_2},见式(11).

$$\mu = \frac{\theta}{\alpha_{N_2} + \beta_{N_2}}; \tag{10}$$

$$D_{N_2} = \frac{\mu(\alpha_{N_2}) + \Delta\alpha_{N_2}}{\mu(\alpha_{N_2} + \beta_{N_2}) + \Delta\alpha_{N_2} + \Delta\beta_{N_2}}, \tag{11}$$

式中:$\Delta\alpha_{N_2}$、$\Delta\beta_{N_2}$ 分别为节点 N_2 在最近 Δt 内正常通信行为和恶意通信行为的行为增量.

$$\Delta\alpha_{N_2} = \sum_{k=1}^{x} n_k, \tag{12}$$

式中:x 为 Δt 内所有记录节点 N_2 通信行为的成员节点;n_k 为各成员节点记录节点 N_2 在 Δt 内正常传输数据的次数,累加求和得出 $\Delta\alpha_{N_2}$ 为簇头统计得出节点 N_2 在 Δt 内正常通信行为总次数.

$$\Delta\beta_{N_2} = \sum_{k=1}^{x} m_k, \tag{13}$$

式中:m_k 为各成员节点记录节点 N_2 在 Δt 内恶意行为次数,通过时间序列的融合、匹配,判断节点的行为,累加求和得出 $\Delta\beta_{N_2}$ 为簇头统计得出节点 N_2 在 Δt 内恶意通信行为总次数.

簇头统计计算出各节点的信誉值,主观设定信誉阈值 δ,当簇内节点信誉值低于信誉阈值,则簇头广播通知簇内节点将该节点加入通信黑名单,将各节点信誉值发送到汇聚节点,以便于信誉值的跨簇查询. 模型的工作流程图如图 3 所示.

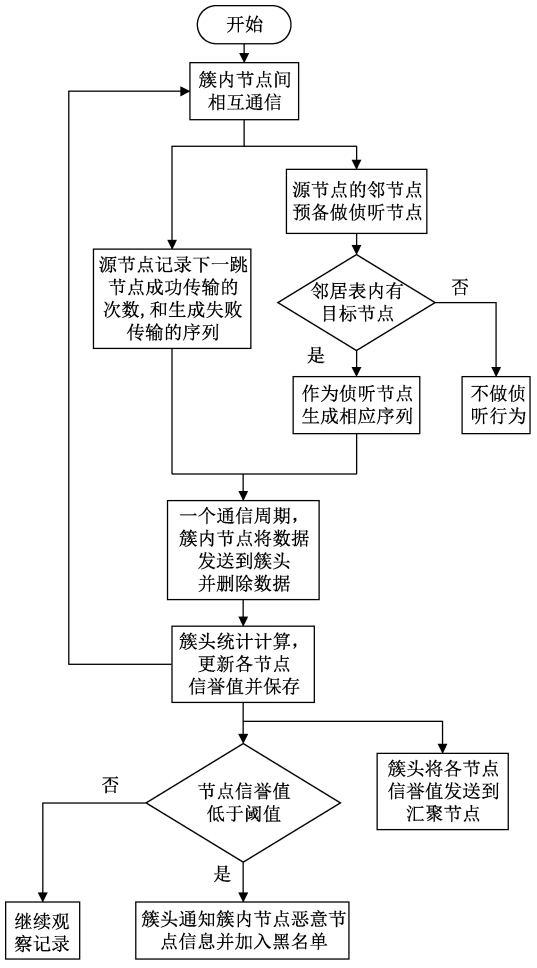

图 3　模型工作流程图

Fig. 3　Model workflow chart

2　仿真与分析

采用 MATLAB2016a 搭建仿真环境,仿真环境设置:100 m × 100 m 的正方形区域随机分布 100 个节点,分 4 个簇,节点通信半径为 20 m. 环境参数设为 0,加入信道冲突概率设为 0.1,除去失效节点和故障节点,正常节点以百分百相应通信请求. 恶意节点以 0.9 的概率不合作通信请求(仿真参数如表 1,初始节点分布见图 4).

表 1　仿真参数

Tab. 1　Simulation parameters

仿真区域/m	节点个数	节点初始信誉值	分簇内节点数量	通信半径/m	节点通信请求发送次数/(贝·s^{-1})	信誉刷新周期/s
100 × 100	100	0.5	25	20	100	60

2.1　节点信誉值变化

仿真实验中节点的信誉值变化情况如图 5,其中节点 N_{d1}、N_{d2} 为恶意节点,N_{d3} 为正常节点,N_{d4} 是有恶意侦听时的正常节点. 图 5 显示恶意节点的信誉值从初始开始逐渐下降,经过 4 个采样周期后在信誉值趋近于 0.1. 正常节点的信誉值则逐步上升,并趋近于 1,而当存在诽谤攻击时,正常节点的信誉值上升相对缓慢,经过 4 个采样周期后,信誉值也趋近于 1.

2.2　维护值 θ 对信誉值的影响

正常节点中途遭遇攻击时,节点信誉值的变化如图 6 所示. 环境参数设为 0,信道冲突概率设为 0.1,采样周期为 100 轮,恶意节点以 0.9 的概率不合作,其他参数参照表 1. 图 7 为当存在环境因素影响时,维护值 θ 对模型误检率的影响.

由图 6 可知,当节点在第一个采样周期受到攻击后,维护值越小,信誉值的收敛速度越快. 由图 7 可知,当环境因素影响越大,维护值越小,模型检测的误差率越大. 当环境因素为 0.25,维护值为

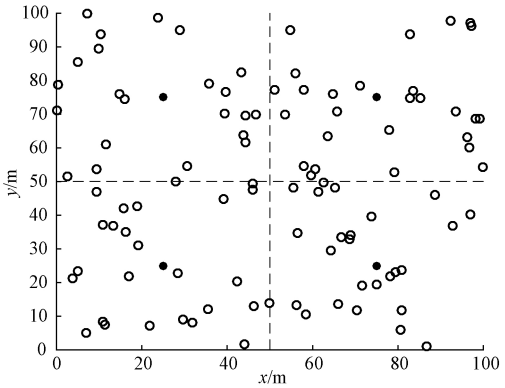

图 4 初始节点分布

Fig. 4 Initial node distribution

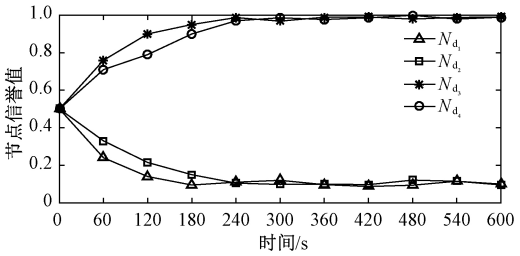

图 5 节点信誉值

Fig. 5 Node reputation value update

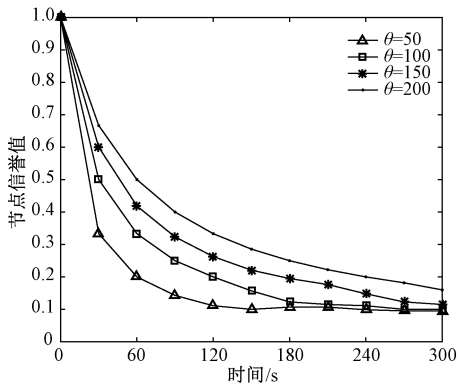

图 6 θ 对信誉值影响

Fig. 6 The influence of θ on the reputation value

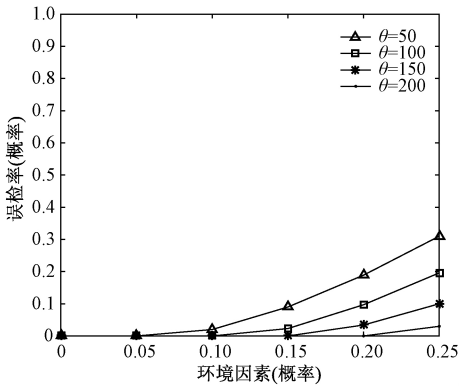

图 7 不同环境因素下 θ 对误检率的影响

Fig. 7 The effect of different environmental factors on the false detection rate of θ

150 时,模型的误检率在所能接受的范围内. 所以不同的环境因素应当选定相应的维护值,以得到更快的收敛速度降低恶意节点对网络的影响.

2.3 安全性能分析

关于无线传感器的安全性能,各节点的信誉值是最直观的评价. 若节点信誉值低于先前预设的信誉阈值,则可以判定该节点为恶意节点,进行标记并由簇头节点和 SINK 节点对整个网络内节点进行广播通知. 当传感器网络中恶意节点数量增多,能否快速、准确、有效地识别恶意节点,是辨别信誉模型安全性能的重要标准. 笔者将恶意节点的不合作概率设为 0.8,信誉阈值设为 0.3,信道冲突概率设为 0.1,其他参数参照表 1,与文献[7]置信度模型以及文献[8]RD-HBRS 模型进行安全性能比较,来对比各模型对恶意节点的识别能力(见图 8 和图 9).

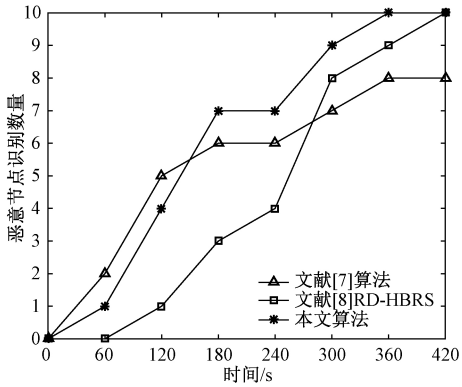

图 8 恶意节点识别数

Fig. 8 Number of malicious nodes

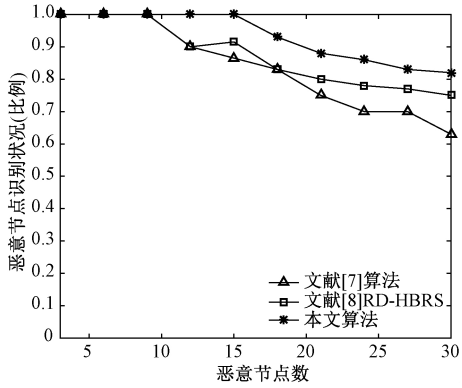

图 9 恶意节点识别率

Fig. 9 Malicious node recognition rate

由图 8 可知,文献[7]置信度模型因为收集大量信誉信息,采样初期识别速度略快于 TS-BRS 模型,文献[8]RD-HBRS 模型因为采用了去冗余机制,初期识别恶意节点效率不足. 而到采样中期 TS-BRS 模型由于降低了误检率,恶意节点识别效率明显优于其他两种模型. 由图 9 可知,当网络内恶意节点数量不断增多,TS-BRS 模型通过时间序列对节点行为的具体表述,解决因为信道占用问题而产生的误差影响,对于恶意节点的识别率明

显高于其他两种算法.

3　结论

在基于 RD-HBRS 模型以簇头为中心的分层信誉值管理的基础上,取消了传统模型中第三方信誉评价,引入了目标节点状态行为时间序列以及通信行为时间序列,通过簇头将信息融合统计,得到了相应时间点内目标节点的行为判定,降低了因为网络拥堵所产生的信道占用而使得信誉模型产生误判. 同时引入维护函数,完善信誉值模型,使得被捕获节点可以快速降低其信誉值,降低其对网络产生的负面影响. 经仿真实验结果表明,TS-BRS 信誉评价模型能够有效地提升网络的安全性能,更快、更有效地识别恶意节点. 主观阈值设定并不适应复杂的传感器网络,下一阶段将对适应性信誉阈值和亚攻击节点识别进行研究.

参考文献:

[1] MOOSAVI H, BUI F M. A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks[J]. Information forensics & security IEEE transactions on, 2014, 9(9):1367 – 1379.

[2] 李建坡,钟鑫鑫,徐纯. 无线传感器网络静态节点定位算法综述[J]. 东北电力大学学报,2015,35(2):52 – 58.

[3] 阎新芳,严晶晶,冯岩. WSN 中基于梯度和粒子群优化算法的分级簇算法[J]. 郑州大学学报(工学版),2016, 37(2):33 – 36.

[4] GANERIWAL S, SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks[C]//Proceeding of the 2nd ACM Workshop on Security of AD Hoc and Sensor Networks. New York: ACM, 2004: 66 – 77.

[5] 盛燕. 无线传感器网络恶意节点识别技术研究[D]. 哈尔滨工程大学信息与通信工程学院,2008.

[6] 杨光,印桂生,杨武. 无线传感器网络安全路由算法的研究与设计[J]. 计算机科学,2008,35(5):55 – 59.

[7] 陈志奎,訾冰洁,姜国海,等. 基于信任云的无线传感器网络信任评估[J]. 计算机应用,2010,30(12):3346 – 3348.

[8] OUYANG X, TIAN B, LI D, et al. A novel hierarchical reputation model for wireless sensor networks[J]. International journal of digital content technology and its applications, 2012, 6(10):61 – 69.

[9] OUYAN X, LI D, ZHANG J Y, et al. Malicious node detection in wireless sensor networks using time series analysis on node reputation[J]. Journal of convergence information technology, 2012, 7(15):8 – 16.

[10] 崔慧,潘巨龙,闫丹丹. 无线传感器网络中基于安全数据融合的恶意节点检测[J]. 传感技术学报,2014,27(5):664 – 669.

[11] 韩挺,罗守山,辛阳,等. 基于动态邻接信任模型的安全路由算法研究[J]. 通信学报,2013,34(6):191 – 200.

[12] 邬春明,杨文月,程亮. 基于 ZigBee 的智能家居温湿度监测系统设计[J]. 东北电力大学学报,2012,32(4):14 – 17.

[13] 阎新芳,张晓丹,严晶晶,等. WSN 中基于离散人工鱼群的分簇拓扑优化算法[J]. 郑州大学学报(工学版), 2017, 38(4):69 – 72.

WSN Bayes Reputation Evaluation Model Based on Time Series Information Analysis

TENG Zhijun[1], GUO Liwen[1], LÜ Jinling[1], HOU Yanquan[2]

(1. Department of Information Engineering, Northeast Electric Power University, Jilin 132012, China; 2. State Grid Qitaihe Electric Power Supply Company, Qitaihe City, Heilongjiang Province 154600, China)

Abstract: In order to effectively reduce the influence of channel occupancy on the reputation evaluation of nodes, and to improve the accuracy of the reputation model, to tackle the data interrupt attacks and selective forwarding attacks, a TS-BRS reputation model was presented based on time series information analysis to evaluate the behavior of nodes. Considering the influence of channel state on network node behavior time series and channel state time series. And the adaptive maintenance function μ was also introduced to update reputation value, add the influence of node behavior on reputation value in reappearing stage, and improve the adaptability of evaluation model. The simulation results showed that the new reputation evaluation model could effectively improve the detection rate and detection speed for malicious nodes. The reputation value of a malicious node could converge more quickly.

Key words: wireless sensor network; time series; bayesian theory; reputation evaluation; channel