一种基于灰色马尔可夫模型的信誉评测模型及其安全路由协议*

曾梅梅, 蒋 华, 王 鑫, 刘伟强
(桂林电子科技大学 计算机科学与工程学院, 广西 桂林 541004)

摘 要: 针对无线传感器网络信誉评测机制不全面,可能造成误判节点信誉值的行为,设计一种基于灰色马尔可夫模型的信誉评测模型,并针对该模型设计一种查询路由协议,解决路由协议中存在选择性转发攻击的问题。基于灰色马尔可夫信誉评测模型是通过改进 BRSN 模型,综合考虑节点通信行为和评价行为的直接信誉、间接信誉、历史信誉以及能量信誉,使用灰色马尔可夫模型对节点的当前信誉与历史信誉进行纵向分析,提高信誉评测模型的精确度。此外,将该模型的节点综合信誉应用于路由选择,设计一种能量高效的查询路由协议,从而提高查询路由协议的安全性。实验表明,该信誉评测模型的节点信誉分布情况符合节点类型,且误判率较低;该查询路由协议的路由安全性较高,能耗性较低,因此无线传感器网络安全路由协议的整体性能都得到了提高。

关键词: 信誉评测; 历史信誉; 灰色马尔可夫模型; 安全路由协议
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2013)12-3758-04
doi:10.3969/j.issn.1001-3695.2013.12.062

Reputation evaluating model and security routing protocol of wireless sensor networks based on grey Markov model

ZENG Mei-mei, JIANG Hua, WANG Xin, LIU Wei-qiang
(*School of Computer Science & Engineering, Guilin University of Electronic Technology, Guilin Guangxi* 541004, *China*)

Abstract: For reputation evaluation mechanisms of WSNs was not comprehensive, it may cause the miscarriage justice behavior of the node reputation value, therefore this paper designed a reputation eva-luation model based on gray Markov model and a query routing protocol designed for this model to solve the routing protocol of selective forwarding attack. The reputation evaluation model based on gray Markov improved BRSN model, and comprehensively considerated direct reputation, indirect reputation, history reputation of the node communication behavior and evaluation behavior and energy reputation, and then used gray Markov model to vertically analyze the node's current reputation and historical reputation to improve the accuracy of reputation evaluation model. In addition, it used the node comprehensive reputation of the model in routing to design an energy efficient query routing protocol to improve the security of the query routing protocol. The experiments show that node reputation distribution of the reputation evaluation model is in line with node-type, and have low rate of false positives; the query routing protocol have higher security, lower energy consumption, so the overall performance of the WSNs secure routing protocol are improved.

Key words: reputation evaluating; history reputation; gray Marko model; secure routing protocol

无线传感器网络由于自身通信的特殊性,将导致其易受多种攻击,因此提高传感器节点的能量利用率和网络安全性的任务至关重要[1]。信誉评测机制作为密码安全机制的一个重要补充,它能够显著地抵御内部威胁,成为抵御内部威胁的重要方法之一,也是学术界研究的一个热点。根据信任证据的种类划分,无线传感器网络的信任管理系统分为基于授权的信任管理系统和基于行为的信任管理系统两类。其中,基于授权的信任管理系统根据部署前的预置凭证决定个体之间的信任关系,两个不相关的个体也可以通过信任链或委托授权的方法实现信任传递。但是该类方法存在授权个体权利过大的缺点,一旦授权个体被俘虏,整个网络就可能瘫痪,而且对内部攻击的防御较弱,因此不适于无线传感器网络。基于行为的网络信任管理系统通过监测节点的行为,建立适当的计算模型而获得对被评测节点的信任值。该类方法占用资源相对较少、无授权中心等特点,适用于无线传感器网络。当前无线传感器网络的信任管理研究主要集中在基于节点行为的信任管理系统[2]。

1 相关研究

目前,已有大量的研究工作从不同角度展开,旨在延长网络生命周期和提高网络安全传输指数。文献[3]针对无线传感器网络的信誉管理系统进行深入研究和分析,并介绍信誉评测机制的特点、分类方法、脆弱性、攻击模型以及安全策略等。文献[4]提出一种基于节点行为与 D-S 证据理论的传感器网络信任评估方法,根据节点的行为来决定信任因子的值,如收

收稿日期: 2013-04-26; **修回日期**: 2013-06-17 **基金项目**: 国家自然科学基金重点资助项目(61262074)

作者简介: 曾梅梅(1989-),女,福建莆田人,硕士研究生,主要研究方向为无线传感器网络安全(zmmmmz123@163.com);蒋华(1963-),男,教授,博士,主要研究方向为网络信息安全;王鑫(1976-),男,副教授,硕士,主要研究方向为物联网安全、无线传感器网络安全;刘伟强(1987-),男,硕士研究生,主要研究方向为无线传感器网络协议.

包率、发送成功率、转发率、时间粒度等信任因子,然后采用D-S证据理论对其进行综合计算,得出一个综合信誉。文献[5]提出一种 VH-GEAR 安全路由协议采用横向和纵向信任机制相结合的 VH-BRSN 评测模型,改善信誉误判的情况,从而提高路由协议安全性。但是该方案采用的间接信誉是由其他节点直接提供的,存在第三方恶意节点以良好的通信行为获得高信誉值,将导致对正常节点进行诽谤、诬陷等攻击。文献[6]提出一种 MA&TP-BRSN 信誉评估模型,即采用对特定节点进行测评以及侧重于消除第三方节点的恶意诽谤影响。该模型综合考虑网内节点的多种内部攻击行为和自私行为,并给出对应于各类攻击的节点信任值计算和整合的方法,但是在计算过程中忽略节点能量的变化,可能造成节点信誉高但能量已经无法支撑其继续充当路由的重任。文献[7]提出一种综合直接信誉、间接信誉和能量信誉的评估机制,计算出节点的综合信誉评估值,但是对节点历史信誉值没有作出一些综合判断,将使节点信誉值误判率较高。

本文在 BRSN[8] 的基础上,针对网络环境、攻击行为等因素的复杂性、多变性,综合考虑直接信誉、间接信誉以及历史信誉的获取,引入灰色马尔可夫模型对节点信誉进行纵向分析,同时结合能量信誉设计 GMM-BRSN 信誉评测模型,并针对该模型设计一种安全查询路由协议 GMM-EESR,有效解决查询路由协议存在的选择性转发攻击问题。

2　解决方案

2.1　能量信誉

传感节点的能量限制性,因此将节点的能量作为计算信誉的因素之一。节点的能量信誉评估值[9] 如式(1)所示:

$$ER_{uv}=\begin{cases}\dfrac{E_u}{E} & ET_{uv}\geqslant\theta\\ 0 & ET_{uv}<\theta\end{cases}\qquad ET_{uv}=\frac{E_u}{(E_{T_x}+E_{R_x})}\tag{1}$$

其中:E_u 表示节点 u 现有能量;E 表示节点初始化能量;E_{T_x} 表示节点 u 到 v 间通信能量;E_{R_x} 表示节点 u 收到数据所耗的能量;ET_{uv} 是节点 u 到 v 的能量信任评价;θ 表示能量阈值。当节点 u 的能量信誉参数 $ET_{uv}\geqslant\theta$ 时,则表示节点 u 能量可信,能量评估值为 E_u/E;相反则认为节点 u 能量不可信,能量评估值置为 0。

2.2　节点行为信誉评测

GMM-BRSN 信誉评测包括直接信誉和间接信誉,并对信誉进行横向和纵向分析,最终获得一个更为精确的节点综合信誉。

2.2.1　直接信誉

直接信誉的信誉因素主要包括节点的通信行为和评价行为的评价。其中,通信行为的评价是根据节点多跳确认机制,通过路径中所有节点在接收到数据包后,都将产生一个相应的 ACK 包并向相反路径发送,而且该 ACK 包必须根据数据包进行认证生成一个 MAC 码。假设节点 u 与邻居节点 v 的正常通信行为次数为 α_{uv_d},节点 u 与邻居节点 v 的异常通信行为次数为 β_{uv_d},节点 u 对节点 v 直接信誉表示为(α_{uv_d},β_{uv_d})。以图 1 为例,假设节点 S 生成一个数据包并发送到 sink 节点:a)初始化每个节点的直接信誉(0,0),并把数据包沿着路径传递到 n_1,这时 n_1 要向节点 S 传送一个相应的认证包 ACK_{1s};b)n_1 沿着路由路径传递给 n_2,这时 n_2 要根据数据包内容生成两个相应的认证包 ACK_{2s}、ACK_{21},随后反向传递到 n_1 和 S;c)以此类推。当节点成功收到一个 ACK 包时,就对评测节点相应的信誉值 α_{uv_d}加 1,反之 β_{uv_d}减 1。一定时间间隔内,邻居节点发送的数据包数量,如果超过设定的上限,则邻居节点可能进行 DoS 攻击;如果没有达到设定的下限值,则该节点可能是自私节点,出现以上情况分别对其节点的信誉值 β_{uv_d}减 1。

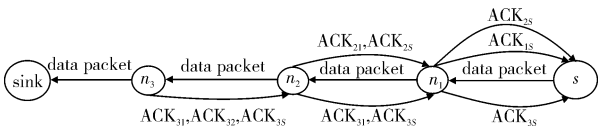


图 1　节点多跳确认机制示意图

评价行为的评价,根据同一邻域内的节点对同一个节点通信行为的评价差值不会相差太多,即 $|C_{uk}-C_{vk}|\leqslant\theta(u,v,k\in\delta_{uv},\theta$ 为一个大于零的小数量值,δ_{uv} 为节点 u 关于节点 v 的邻域),从而建立对节点 v 的评价行为检测规则和参数统计规则[6],如式(2)所示:

$$\begin{cases}\alpha'_{uv\_d}=\alpha'_{uv\_d}+a & |C_{uk}-C_{vk}|\leqslant\theta\\ \beta'_{uv\_d}=\beta'_{uv\_d}+b & |C_{uv}-C_{vk}|>\theta\end{cases}\quad\theta\in(0,1)\tag{2}$$

其中:a 表示节点对评价行为正常行为次数的统计更新;b 表示节点对评价行为异常行为次数的统计更新。当节点 u 接收到节点 v 对节点 k 的通信行为评价时,比较自身和节点 v 分别对节点 k 通信行为之间的差值,如果小于 θ,则对 $\alpha'_{uv\_d}+1$,否则 $\beta'_{uv\_d}-1$。

2.2.2　间接信誉

间接信誉是节点通过信誉信息交换,从第三方节点获得的信誉。由于存在第三方恶意节点通过良好通信行为来提高自己信誉,存在对正常节点进行抵毁的行为,本文以第三方节点的评价行为和通信行为作为获取间接信誉的因素。基于 JoSANG 信任原理[10],采用 TP-BRSN[6] 方案,综合考虑第三方节点通信行为和评价行为的好坏。

通过一个三元组(b,d,u)对信息真实性的信任程度进行描述。其中,b 表示可信(belief),d 表示不可信(disbelief),u 表示不确定(uncertainty)三个信任级别,以及 $b,d,u\in[0,1]$ 且 $b+d+u=1$。元组(b,d,u)与 Beta 分布(Beta(α,β))参数之间的映射关系如式(3)所示:

$$\begin{cases}b=\dfrac{\alpha}{\alpha+\beta+2}\\ d=\dfrac{\beta}{\alpha+\beta+2}\\ u=\dfrac{2}{\alpha+\beta+2}\end{cases}\tag{3}$$

假设元组($b_{uk\_d},d_{uk\_d},u_{uk\_d}$)表示节点 u 对节点 k 通信行为的直接信任评价;元组($b'_{uk\_d},d'_{uk\_d},u'_{uk\_d}$)表示节点 u 对节点 k 评价行为的直接信任评价;元组($b_{kv\_d},d_{kv\_d},u_{kv\_d}$)表示在节点 k 传递给节点 u 的信息中节点 k 对节点 v 通信行为的间接信任评价;元组($b^k_{uv\_\mathrm{ind}},d^k_{uv\_\mathrm{ind}},u^k_{uv\_\mathrm{ind}}$)表示节点 u 通过第三方节点 k 提供的关于节点 v 的信息而达成的对节点 v 的通信行为的评价,如式(4)所示,有如下关系存在:

$$\begin{cases}b^k_{uv\_\mathrm{ind}}=b'_{uk\_d}b_{uk\_d}b_{kv\_d}\\ d^k_{uv\_\mathrm{ind}}=b'_{uk\_d}b_{uk\_d}d_{kv\_d}\\ u^k_{uv\_\mathrm{ind}}=d'_{uk\_d}+u'_{uk\_d}+b'_{uk\_d}(d_{uk\_d}+u_{uk\_d})+b'_{uk\_d}b_{uk\_d}u_{kv\_d}\end{cases}\tag{4}$$

将式(3)代入式(4),可得通信行为的间接信誉的 Beta 分布($\alpha^k_{uv\_\mathrm{ind}},\beta^k_{uv\_\mathrm{ind}}$),如式(5)所示,同理可得评价行为的 Beta 分布($\alpha^{k'}_{uv\_\mathrm{ind}},\beta^{k'}_{uv\_\mathrm{ind}}$)。

$$\begin{cases} \alpha_{uw\_\mathrm{ind}}^{k} = \dfrac{2\alpha_{uk\_d}\alpha'_{uk\_d}\alpha_{kv\_d}}{[(\beta'_{uk\_d}+2)(\alpha_{uk\_d}+\beta_{uk\_d}+2)+\alpha'_{uk\_d}(\beta_{uk\_d}+2)](\alpha_{kv\_d}+\beta_{kv\_d}+2)+2\alpha_{uk\_d}\alpha'_{uk\_d}} \\ \beta_{uw\_\mathrm{ind}}^{k} = \dfrac{2\alpha_{uk\_d}\alpha'_{uk\_d}\beta_{kv\_d}}{[(\beta'_{uk\_d}+2)(\alpha_{uk\_d}+\beta_{uk\_d}+2)+\alpha'_{uk\_d}(\beta_{uk\_d}+2)](\alpha_{kv\_d}+\beta_{kv\_d}+2)+2\alpha_{uk\_d}\alpha'_{uk\_d}} \end{cases} \tag{5}$$

在对节点行为信誉整合时应该重视自身的监测结果，部分采纳他人的经验，因此各行为节点的信誉整合如下：

对通信行为的直接信誉和间接信誉进行整合，如式(6)所示，同理可得，对评价行为的直接信誉和间接信誉进行整合。

$$\begin{cases} \alpha_{uw} = \omega_1\alpha_{uw\_d} + \omega_2\alpha_{uw\_\mathrm{ind}} \\ \beta_{uw} = \omega_1\beta_{uw\_d} + \omega_2\beta_{uw\_\mathrm{ind}} \end{cases} \tag{6}$$

其中：ω_1、ω_2 为权值，$\omega_1+\omega_2=1$ 且 $\omega_1>\omega_2$。

2.2.3 当前信誉评测

将 BRSN 对信誉分布与 Beta 分布进行拟合分析，可得 Beta(α_{uw},β_{uw})分布能够描述节点信誉的分布，如式(7)所示，其中 C_{uw} 为节点 u 关于邻居节点 v 的信誉分布。

$$C_{uw} \sim \mathrm{Beta}(\alpha_{uw},\beta_{uw}) \tag{7}$$

通过计算信誉分布的统计期望来得到节点的信誉 R_{uw}，如式(8)所示。其中，通信行为的当前信誉评测 CTR 如式(9)所示，同理可得，评价行为的当前信誉评测 CAR。

$$R_{uw} = E(C_{uw}) = E(\mathrm{Beta}(\alpha_{uw}+1,\beta_{uw}+1)) = \frac{\alpha_{uw}+1}{\alpha_{uw}+\beta_{uw}+2} \tag{8}$$

$$\mathrm{CTR} = \frac{\omega_1\alpha_{uw\_d}+\omega_2\alpha_{uw\_\mathrm{ind}}+1}{\omega_1\alpha_{uw\_d}+\omega_2\alpha_{uw\_\mathrm{ind}}+\omega_1\beta_{uw\_d}+\omega_2\beta_{uw\_\mathrm{ind}}+2} \tag{9}$$

2.3 信誉纵向分析

本文采用灰色马尔可夫模型(grey Markov model, GMM)[11]进行预测。灰色理论对节点信誉评测时，具有处理样本少、计算量小、模糊性数据、随机性动态变化、预测准确度高的优势，擅长于非线性评测，专门适用于预测小样本、贫信息不确定性系统。但是节点信誉可能遭受外界因素影响，导致随机波动性大、变化趋势多样性、复杂性等问题，因此采用马尔可夫理论的状态转移矩阵对灰色模型评测结果进行完善。

在灰色 $GM(1,1)$ 预测过程中，首先建立时间趋势的 $GM(1,1)$ 模型，即对 $n-1$ 个的历史信誉 $r(t_k)(k=1,2,\cdots,n-1)$ 的时间序列 $R(t)=\{r(t_1),r(t_2),\cdots,r(t_{n-1})\}$ 进行累加变换获得递增时间序列 $\hat{R}(t)$，对其建立微分方程并求解，得出随时间序列变化函数 $F(t)$，求得与历史信誉 $r(t_k)(k=1,2,\cdots,n-1)$ 对应的预测值 $\hat{r}(t_k)(k=1,2,\cdots,n-1)$，计算出这两个值之间的残差 $e(t_k)=r(t_k)-\hat{r}(t_k)(k=1,2,\cdots,n-1)$，并将其按时间顺序构成信誉残差系列 $\hat{E}(t)=\{e(t_1),e(t_2),\cdots,e(t_{n-1})\}$。

然后针对灰色模型存在的局限，通过马尔可夫状态概率矩阵的误差进行修正。修正步骤如下：a)进行状态划分，根据历史信誉残差序列 $\hat{E}(t)=\{e(t_1),e(t_2),\cdots,e(t_{n-1})\}$ 中的最大值 $e_{\max}$ 和最小值 $e_{\min}$，将序列划分为若干个状态区间；b)建立状态转移概率，根据 $e(t_k)(k=1,2,\cdots,n-1)$ 所处的状态，通过对相邻时刻 $e(t_k)$ 所处的状态变化的统计，计算出在 $e(t_k)$ 各个状态之间的转移概率，建立状态转移矩阵；c)计算预测值，根据当前时刻 $e(t_{n-1})$ 所处状态，结合状态转移概率矩阵判断出 n 时刻残差 $e(t_n)$ 最有可能存在的状态，以该状态区间的中间值为 $e(t_n)$ 的取值，对 $GM(1,1)$ 模型预测的 n 时刻的风险值进行误差修正，得到灰色马尔可夫模型对 n 时刻的节点信誉值 $\hat{r}'(t_n)=\hat{r}(t_n)-e(t_n)$。

第 n 时刻，纵向和横向分析相结合的节点信誉值，如式(10)所示：

$$\mathrm{VHR}_n = \omega CR_n + (1-\omega)\hat{r}'(t_n) \tag{10}$$

其中：ω 为当前信誉的权重。

2.4 综合信誉

评价行为信誉 AR、通信行为信誉 TR 与能量信誉 ER 的整合，如式(11)所示：

$$R = (f_1\times ER + f_2\times TR + f_3\times AR)\times V_I \tag{11}$$

其中：V_I 是由入侵检测系统列出的恶意节点表；1 为正常节点，0 为恶意节点；f_1、f_2、f_3 表示权值，可以根据网络具体要求来设不同的值，f_1、f_2、$f_3\in[0,1]$ 且 $f_1+f_2+f_3=1$。

2.5 信誉更新机制

针对信誉更新机制，本文采用设置定时器周期性触发更新信誉，避免节点频繁更新信誉，从而优化网络能耗并延长网络生命周期。周期性信誉更新机制是通过在邻居节点配置定时器进行实现。具体步骤如下：

a)安装信誉更新定时器。在节点周围的所有邻居节点都安装上信誉更新定时器，并启动。

b)更新信誉。当到达定时器设置的时间，节点先从邻居节点中获取最新的信息；然后信誉对象根据最新信息进行 GMM-BRSN 节点信誉评测，包括对节点的信誉和能量值的评测，最后得到综合信誉。

c)定时器返回。信誉更新完成，定时器需要重新返回。为达到信誉值能够周期性更新，把定时器设置成三种返回状态：(a)当更新周期不变时，返回值为 0；(b)当需要重设更新周期时，返回值大于 0，即新周期值；(c)当不再获取该节点的信誉更新时，返回值小于 0。信誉更新定时器会随着邻居节点的消失而失效。

3 路由构造

为了降低能量损失，该路由协议中的节点管理采用休眠与调用机制。

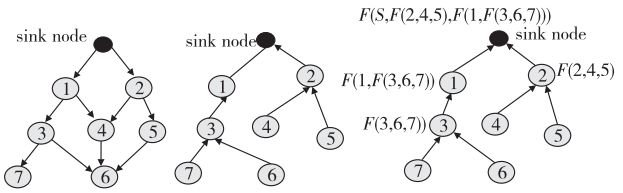
a)当网络中的节点收到查询消息 Q 后，需要把该节点到 sink 节点的路由信息全部添加到消息 Q 上，并继续广播消息 Q，直到网络中所有的节点都能够获取到其与 sink 节点通信的路由信息。为了减少广播消息 Q 带来的能耗，节点在收到路由信息后进行判断，比较路由跳数与该节点收到的其他路由消息中的路由跳数。如果前者大于后者，则丢弃该广播消息，反之则保留。

b)广播过程结束后，所有节点的路由表都各自存有其到 sink 节点的最短路由信息。

c)根据上章所述的综合信誉值 VHR，在邻居列表中选择 sink 节点综合信誉值最高的邻居节点时，首先判断节点的行为信誉值或能量信誉值是否小于设定的阈值。如果小于，则将该警告信息广播到全网中的其余节点，同时把该邻居节点排除，继续寻找下一个邻居节点；否则计算该邻居节点到 sink 节点的综合信誉值。如果该节点到 sink 节点的综合信誉值大于初始信誉值，则将当前信誉值作为最大信誉值，并且更新路由表中的节点 ID，即选择其作为上游节点(父亲节点)，同时向其子孙节点发送消息；否则继续计算其余的邻居节点，直到遍历完所有邻居节点。

d)将生成以 sink 节点为根节点的信誉最高生成树，即最

优路由路径,然后传感器节点将感知数据传送到父亲节点。父亲节点对其所收到的所有数据进行融合,从而减少数据通信量,最后把融合数据包传递到 sink 节点,如图 2 所示。



(a)sink node 广播消息　(b)最大生成树形成　(c)查询结果融合并传递到sink node

图 2　路由构造步骤示意图

4　实验仿真与分析

实验在 Windows 7 环境下,采用 CYGWIN + NS2 的仿真软件,对算法进行验证。仿真实验的网络场景如下:100 个节点分布在一个 800 m × 800 m 矩形区域,sink 节点在传感器区域外任意位置,通信半径为 200 m,在部分实验中会对个别节点的位置作适当调整。

1)GMM-BRSN 信誉分布

验证正常节点(normal node)、意外丢包节点(accidental node)和恶意节点(malicious node)三类节点在 GMM-BRSN 信誉评测模型中的信誉分布情况。仿真时间为 1 600 s,信誉更新周期为 100 s,恶意节点丢包率为 85%,意外丢包节点丢包率为 80%,意外丢包时长为 200 s(500 s ~ 700 s),灰色马尔可夫纵向分析的当前信誉权重 ω 为 0.6。仿真结果如图 3 所示,表明恶意节点的信誉随仿真时间的推移,最后保持在一个低信誉值;意外丢包节点的信誉不稳定,尤其是在 500 s ~ 700 s,信誉先是急剧下降,然后缓慢恢复平稳,这是因为 GMM-BRSN 信誉评测模型采用纵向历史评测,可以平衡意外丢包带来的短期波动,所以节点信誉只会发生小幅度的减弱,并在行为正常后信誉逐渐恢复到原来的信誉,有效地解决了节点由于环境原因产生的非法数据引起低信誉的问题;正常节点伴随着仿真时间的推移一直平稳地保持在一个高信誉的位置。因此,GMM-BRSN 信誉评测模型能够根据信誉分布曲线情况识别不同类型节点。

2)意外丢包节点信誉分布

分析意外丢包节点在 BRSN、I-BRSN 和 GMM-BRSN 三种信誉评测模型中的信誉分布情况。仿真结果如图 4 所示,表明 GMM-BRSN 对意外丢包节点信誉曲线比较平滑,说明 GMM-BRSN 对意外节点丢包的容忍性最强,而且不影响信誉的整体变化趋势,避免对意外丢包节点误判的情况。

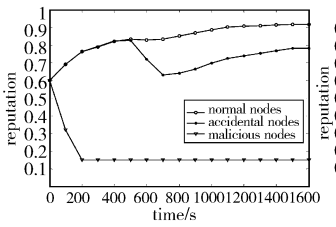


图 3　不同类型节点的信誉分布情况

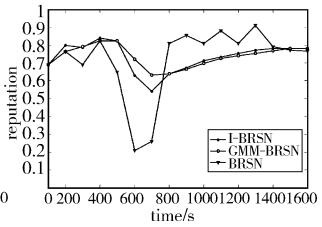


图 4　意外丢包节点在不同信誉评测模型中的信誉分布

3)GMM-EESR 误判率

分析不同的当前信誉权值 0.5、0.6、0.7 对 GMM-EESR 路由协议中意外丢包节点的误判率。意外丢包节点个数分别从 0 开始每次递增 3 个直到 27 个。仿真结果如图 5 所示,表示权值取 0.6 的 GMM-EESR 路由协议,其误判率比较低,表明权值过大或者过小,都不利于对意外丢包节点进行客观评判。

4)GMM-EESR 丢包率

与基于查询路由协议 DD[12] 进行对比实验,分析不同恶意节点数目下路由协议的丢包率情况。仿真结果如图 6 所示,表示随着恶意节点数目的增加,网络的丢包率递增,相比 DD 路由协议,GMM-EESR 路由协议丢包率增加比较缓慢,是因为它能够根据节点信誉值情况选择路由节点,避免恶意节点被选择的可能性,所以网络的丢包率较低。

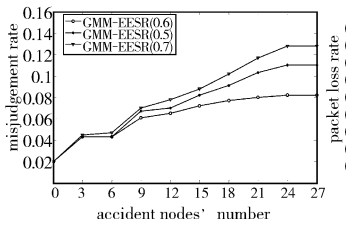


图 5　不同当前信誉权值 ω 误判率对比

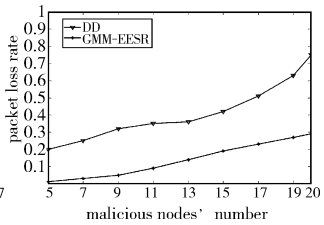


图 6　不同恶意节点数目下的网络丢包率

5)GMM-EESR 能耗率

对比一定时内网络中所有节点的整体能耗率。仿真时间为 1 000 s,能量初始化为 50 J,节点睡眠能耗为 0.001 J,信誉更新周期为 100 s。两种路由协议仿真结果如图 7 所示,表明与 DD 路由协议对比,GMM-EESR 的能耗降低 10%,延长了网络的生命周期。

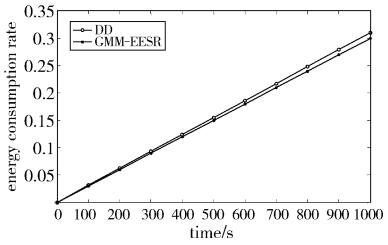


图 7　不同协议能耗率对比

5　结束语

本文主要针对无线传感器网络的信誉评测及安全路由协议问题,设计一种基于节点行为的信誉预测机制及安全路由协议。该协议是基于 BRSN 信誉评测模型,对节点通信行为和评价行为的直接信誉和间接信誉进行横向和纵向分析,并与能量信誉合并成为节点间通信的条件。在路由选择时,优先选择信誉值高的路径,充分考虑到通信过程中的安全和能量问题。但是,目前仅局限于在查询路由协议中,在未来工作中将研究节点数量众多的层次型网络拓扑结构的问题,进一步完善所设计的算法,建立相关的数学模型,扩大算法的适用范围。

参考文献:

[1] CHEN Xiang-qian, MAKKI K, YEN K, *et al*. Sensor network security: a survey[J]. IEEE Communications Surveys & Tutorials, 2009, 11(2): 52-73.

[2] AIVALOGLOU E, GRITZALIS S, SKIANIS C. Trust establishment in sensor networks: behaviour-based, certificate-based and a combinational approach[J]. International Journal of System of Systems Engineering, 2008, 1(1): 128-148.

[3] 荆琦,唐礼勇,陈钟. 无线传感器网络中的信任管理[J]. 软件学报,2008,19(7):1716-1730.

[4] 成坚,冯仁剑,许小丰,等. 基于 D-S 证据理论的无线传感器网络信任评估模型[J]. 传感技术学报,2009,22(12):1802-1807.

(下转第 3766 页)

5 结束语

本文在动态污点分析的基础上,针对非控制数据攻击提出了一个改进的指针污点分析方法,通过跟踪内存数据的污点标记和指针标记,监控是否存在非法的指针解引用,实现了原型工具 DPTA。实验评估表明,该工具可以防御控制数据攻击和大部分非控制数据攻击。虽然 DPTA 实现了本文防御模型,但是还存在一些问题需要进一步研究:

a)实验表明本文原型系统运行效率并不是很理想,距离商业化应用还有距离。笔者计划通过两方面进行优化:一方面优化 Tagmap 的数据结构,更新 Tagmap 信息是系统中常见的操作,因此快速获取 Tagmap 中的信息会对效率产生很大影响;另一方面手动分析程序调用的常用函数的语义信息,获取其是否涉及污点传播,对于不涉及污点传播的函数不进行插桩分析。

b)目前采取的指针识别方法并不是很准确,尤其是静态分配空间的指针,下一步计划分析识别失败的指针,归纳其特征,提高指针识别的准确率。

c)本系统无法检测出不通过覆写指针实施的非控制数据攻击,可以通过结合静态分析的方法防御,但这不是下一步的主要方向。

参考文献:

[1] ROEMER R, BUCHANAN E, SHACHAM H, *et al*. Return-oriented programming: systems, languages, and applications [J]. ACM Trans on Information and System Security, 2012, 15(1): 2.

[2] CHEN Shuo, XU Jun, SEZER E C, *et al*. Non-control-data attacks are realistic threats[C]//Proc of the 14th Conference on USENIX Security Symposium. Berkeley: USENIX Association, 2005: 12.

[3] SLOWINSKA J M. Using information flow tracking to protect legacy binaries[M]. [S. l.]: Vrije Universiteit, 2012.

[4] NEWSOME J, SONG D. Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software [EB/OL]. (2005). http://valgrind.org/docs/newsome2005.pdf.

[5] EGELE M, SCHOLTE T, KIRDA E, *et al*. A survey on automated dynamic malware-analysis techniques and tools[J]. ACM Computing Surveys, 2012, 44(2): 6.

[6] 王蕊,冯登国,杨轶,等.基于语义的恶意代码行为特征提取及检测方法[J].软件学报,2012,23(2):378-393.

[7] 刘杰,王嘉捷,欧阳永基,等.基于污点指针的二进制代码缺陷检测[J].计算机工程,2012,38(24):46-49.

[8] LUK C K, COHN R, MUTH R, *et al*. Pin: building customized program analysis tools with dynamic instrumentation[C]//Proc of ACM SIGPLAN Conference on Programming Language Design and Implementation. New York: ACM Press, 2005: 190-200.

[9] SCHLESINGER C, PATTABIRAMAN K, SWAMY N, *et al*. Modular protections against non-control data attacks[C]//Proc of the 24th IEEE Computer Security Foundations Symposium. 2011: 131-145.

[10] Van ACKER S, NIKIFORAKIS N, PHILIPPAERT P, *et al*. Valueguard: protection of native applications against data-only buffer overflows[M]//Information Systems Security. Berlin: Springer, 2011: 156-170.

[11] BHATKAR S, SEKAR R. Data space randomization[M]//Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin: Springer, 2008: 1-22.

[12] XU Jun, NAKKA N. Defeating memory corruption attacks via pointer taintedness detection[C]//Proc of International Conference on Dependable Systems and Networks. Washington DC: IEEE Computer Socitey, 2005: 378-387.

[13] DALTON M, KANNAN H, KOZYRAKIS C. Real-world buffer overflow protection for userspace & kernelspace[C]//Proc of the 17th Conference on Security Symposium. [S. l.]: USENIX Association, 2008: 395-410.

[14] 汪洁,杨柳.基于蜜罐的入侵检测系统的设计与实现[J].计算机应用研究,2012,29(2):667-671.

[15] SLOWINSKA A, BOS H. Pointer tainting still pointless: (but we all see the point of tainting)[J]. ACM SIGOPS Operating Systems Review, 2010, 44(3): 88-92.

[16] KEMERLIS V P, PORTOKALIDIS G, JEE K, *et al*. Libdft: practical dynamic data flow tracking for commodity systems[C]//Proc of the 8th ACM SIGPLAN/SIGOPS Conference on Virtual Execution Environments. [S. l.]: ACM Press, 2012: 121-132.

[17] Polymorph filename buffer overflow vulnerability[EB/OL]. (2003). http://www.securityfocus.com/bid/7663.

[18] ATPHTTPD buffer overflow exploit code[EB/OL]. (2001). http://www.securiteam.com/exploits/6B00K003GY.html.

[19] SAVOLA P. LBNL traceroute heap corruption vulnerability [EB/OL]. (2000). http://www.securityfocus.com/bid/1739.

[20] DOWD M. Sendmail header processing buffer overflow vulnerability [EB/OL]. http://www.securityfocus.com/bid/6991.

(上接第 3761 页)

[5] YANG Wu, MA Xing-guo, WANG Wei, *et al*. Research on reputation evaluating model for WSN nodes based on vertical and horizontal analysis[C]//Proc of the 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing. Washington DC: EE Computer Society, 2010: 293-296.

[6] 杨光,印桂生,杨武,等.无线传感器网络基于节点行为的信誉评测模型[J].通信学报,2009,30(12):18-26.

[7] 姚红燕,周鸣争,刘涛.一种基于节点行为的无线传感器网络信誉计算模型[J].南通大学学报:自然科学版,2011,10(1):5-9.

[8] GANERIWAL S, BALZANO L K, SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks[J]. ACM Trans on Sensor Networks, 2008, 4(3): 15.

[9] HEINZELMAN W R, CHANDRAKASAN A P, BALAKRISHNAN H. An application specific protocol architecture for wireless microsensor networks [J]. IEEE Trans on Wireless Communications, 2002, 1(4): 660-670.

[10] JSANG A, ISMAIL R. The beta reputation system[C]//Proc of the 15th Bled Electronic Commerce Conference. 2002: 41-55.

[11] 刘念,刘孙俊,刘勇,等.一种基于免疫的网络安全态势感知方法[J].计算机科学,2010,37(1):126-129.

[12] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: attacks and counter measures[J]. Ad hoc Networks, 2003, 1(2): 293-315.