无线自组网中多种节点状态的行为特征及关联分析①

印 敏, 沈 晔, 蒋 磊, 冯 径

(解放军理工大学 气象海洋学院, 南京 211101)

摘 要: 从节点行为对网络安全的影响角度看, 恶意节点将直接导致路由破坏或者毁坏数据. 因此, 在节点行为检测和信任度评估时, 必须首先重点关注其安全性行为特征, 以便降低恶意行为节点的信任值. 归纳了网络中九种常见的节点行为类型, 分析了各行为状态的行为特征, 建立了特征模型, 提出了检测特征参数和关联检测模型. 仿真结果表明, 提出的节点行为检测特征参数和关联检测模型, 在静态及网络变化时, 对不合作节点、恶意节点的行为信任值评估定级均有较高的准确性, 可以有效排除这些节点的网络活动.

关键词: 无线自组网; 节点信任评估; 节点行为检测; 节点行为特征

Multiple node Behaviors Profile and Relevance Analysis in Wireless Self-Organized Networks

YIN Min, SHEN Ye, JIANG Lei, FENG Jing

(College of Meteorology and Oceanography, PLA University of Science and Technology, Nanjing 211101, China)

Abstract: In the angle of networks security effects, malicious node behaviors lead to route failure and data destroy. So node behavior security evaluation is the most important evaluation factor in behavior detection and trust evaluation, which can debase trust value of the malicious nodes. This paper has an analysis on 9 sorts of common node behaviors profile, which presents behavior detection parameters and detection model. The results show that in the static and dynamic network environment it reaches a high detection accuracy and evaluation accuracy which can exclude malicious node from network activity effectively.

Key words: wireless self-organized network; node trust evaluation; node behavior detection; node behavior profile

随着日益多样化的需求与不断进步的科技水平, 无线自组网(Wireless Ad Hoc Networks)技术一直受到学术界与工业界的广泛关注. 从最初提出的抢险救灾、野外勘探与战场通信等应用, 到近些年涌现出的一些新型无线网络架构, 如无线传感器网络(Wireless Sensor Network)、车联网(Vehicular Ad Hoc Networks)与物联网(Internet of Things)等, 都标记有“无线自组织”的烙印. 可以看到, 无线自组网技术已经与人类的生产和生活密不可分.

长期以来, 安全性问题一直是无线自组网研究人员所关注的重要问题, 严重制约其推广应用. 越来越多的学者积极参与到无线自组网信任技术的应用研究中[1-3], 主要研究方向包括信任模型、行为监测、度量标准、信任值定级、信任度计算、应用场景及适应性等. 其中, 行为监测是信任模型中的重要部分, 节点通过直接证据或间接证据, 持续地对其它节点进行信任评价, 以便给恶意行为节点设置较低的信任值, 将其孤立.

但是, 在对节点行为进行检测和评估时, 人们根据通信、数据、能量等不同信任要素, 设计了各种行为检测机制和信任度计算方式. 通信要素以是否进行了信息转发来计算信任值; 数据要素以感知的数据与其它节点是否一致来判定节点是否可信; 能量要素以节点的剩余能量是否能完成正常任务来判定其可信程度, 常用指标有数据包转发率[4,5]、丢包率、分组重传率[6]. 根据以上三种信任度量要素, A. Pirzada[7]将信任

① 基金项目:江苏省自然科学基金(BK20130070);国家自然科学基金(41405024,61371119)

收稿时间:2016-03-07;收到修改稿时间:2016-04-27 [doi:10.15888/j.cnki.csa.005469]

定义为网络中的每个具体操作, 例如控制分组转发的信任、数据分组转发的信任, 根据这些度量选项的直接证据进行信任度评估; Li X. [5]在考虑转发率的时候, 加入了对时间的考虑, 用转发率和窗口转发率度量; Li Yu [8]考虑了剩余能量、时延、时延抖动及其它因素, 提出了一种基于多个判决因子的信任模型; Karthik, N. [9]在计算节点信任值时, 用到了传输范围、分组丢失率、能量消耗、时延、路径最优性、节点位置、跳数、信噪比、误比特率等参数.

尽管如此, 仅以信息是否转发、数据是否一致、剩余能量是否最大作为行为检测的依据, 不足以体现出节点的可信任程度, 因为节点的实际行为是否正常, 是否具有攻击性, 这些比上述通信要素、数据要素、能量要素更直接的反映出该节点在网络中的是否应该被信任.

本文从节点行为对网络安全的影响角度, 归纳了网络中节点的常见行为类型, 分析了各行为状态的行为特征, 建立了特征模型; 分析了各节点行为状态之间的相似性、不同点、关联性; 对多节点行为特征模型的可检测性进行了分析和实验, 该模型可以有效识别和区分大多数不同类别的网络节点行为状态.

1　无线自组网中的节点行为类型及行为特征

1.1 无线自组网中的节点行为类型

根据节点对网络安全性的影响后果, 可将节点的行为状态可分为三类, 分别是: 正常行为、不合作行为、恶意攻击行为.

正常节点是在网络中活跃的、愿意为其他节点转发分组的节点. 不合作节点是自私节点或者休眠节点, 不愿意为其他节点提供路由请求包和数据包的转发, 但自己如果是目的节点, 则正常接收. 恶意行为节点包括实施各种攻击行为的节点, 破坏路由、毁坏数据, 常见攻击包括: 选择性转发、sinkhole 攻击、虫洞攻击、黑洞攻击、女巫攻击、资源耗尽攻击等.

在一个未知的隐含内部变坏节点的网络中, 这些节点有可能是并存的. 而无线自组网节点信任评估的目的就是监测各节点行为, 识别各节点的行为类型并设定信任等级, 信任值低的恶意节点将被整网公布甚至被强制清除, 无法继续参与路由和数据转发, 从而达到节点信任评估和保证网络安全的目的.

以往的文献中有很多关于针对选择性转发、虫洞、女巫、黑洞等攻击检测的专门研究, 目的是准确发现网络中这些攻击行为的存在, 然而目前仍然没有一种有效的机制能同时应对上述攻击. 如果将各种方法简单集成在一起使用, 其计算量和复杂度也不可想象.

我们发现, 尽管恶意节点的攻击种类多种多样, 但是从攻击目的和攻击效果上看, 无非是破坏路由、毁坏数据两类. 破坏路由的结果将导致路由不能正确发现, 毁坏数据的结果导致数据被丢掉、篡改. 从这个角度看, 众多恶意节点的攻击行为表现上有很多相似性和共同性. 而且, 无线自组网安全性是通过选择信任值高的节点参与路由发现和数据转发实现的, 只要被识别出是恶意节点行为, 就会被降低信任等级, 至于是否非得要被精确判断是虫洞攻击还是黑洞攻击还是 sinkhole 攻击, 并没有那么大的必要. 因此, 将恶意行为、自私行为、正常行为区分开来比详细确定恶意攻击类别更为重要.

1.2 无线自组网中节点的行为特征

为了达到区分节点行为的目的, 并考虑行为检测的可执行性, 如表 1 所示, 我们研究了网络中常见的各种网络行为, 分析了各自的行为特征和各行为间的关联性, 以便为行为特征识别奠定基础. 这些行为覆盖了无线自组网中的常见恶意攻击, 主要包括: 正常行为、不合作行为、选择性转发行为、sinkhole 黑洞攻击行为、虫洞攻击行为、女巫攻击行为、反复路由请求行为、大量路由应答行为、发送海量无用信息行为. 其中, 选择性转发、sinkhole 黑洞、虫洞、女巫为最危险的恶意攻击行为, 反复路由请求、大量路由应答、发送海量无用信息为网络资源耗尽型攻击行为.

表 1　网络中各类节点行为特征

行为类型	路由发现阶段			数据发送阶段		
	作为中间节点	作为目的节点	行为特征	作为中间节点	作为目的节点	行为特征
正常节点行为	收到请求包立刻转发	收到请求包立刻应答	路由转发率较高	收到数据包立刻转发	收到数据包立刻应答	数据转发率较高
不合作节点行为	收到请求包不转发	收到请求包立	路由转发率为 0	无法通过该节	收到数据包立刻	数据转发率为 0

			刻应答		点建立路由	应答	
恶意攻击节点行为	选择性转发	收到请求包立刻转发	收到请求包立刻应答	路由转发率较高	丢包	收到数据包立刻应答	数据转发率不高
	Sinkhole、黑洞攻击	回复每个请求包, 吸引路由	收到请求包立刻应答	虚假路由吸引流量	丢包、窃听、篡改	收到数据包立刻应答	某节点数据流量大, 吞吐量、转发率可高可低
	虫洞攻击	有隧道, 吸引路由	收到请求包立刻应答	隧道路由吸引流量	丢包、窃听、篡改	收到数据包立刻应答	某节点数据流量大, 吞吐量、转发率可高可低
	女巫攻击	假冒其他节点吸引路由	收到请求包立刻应答	假冒其他节点吸引流量	丢包、窃听、篡改	收到数据包立刻应答	数据流量汇聚不明显, 某节点吞吐量大
网络资源耗尽行为	反复路由请求	无	无	作为源节点发送路由请求分组频繁	无	无	无
	大量路由应答	无	无	作为源节点发送路由应答分组频繁	无	无	无
	发送海量无用信息	中间节点可正常寻路	目的节点可正常应答	作为源节点频繁占用资源	中间节点可正常转发	目的节点可正常应答	数据吞吐量大, 目的节点可判断信息是否有用

下面详细分析路由发现和数据转发过程中各类节点作为中间节点和目的节点时的行为特征. 这是因为, 恶意节点的目的就是破坏路由或者毁坏数据, 为了达到其目的, 恶意节点必然在这两个过程中留下行为痕迹, 影响某些参数统计量. 由于各类节点作为中间节点和目的节点时的行为是不一样的, 因此需要分别分析.

1) 正常行为

正常节点是在网络中活跃的, 作为中间节点, 愿意为其他节点转发路由请求分组和数据分组; 作为目的节点, 正常接收并返回路由应答.

定义 1. 路由转发率: $R_r = \frac{n_{rf}}{n_{rr}}$, 其中, n_{rf} 为实际转发了的请求包个数, n_{rr} 为需要其转发的请求包个数.

定义2. 数据转发率: $R_d = \frac{n_{df}}{n_{dr}}$, 其中, n_{df} 为实际转发了的数据包个数, n_{dr} 为需要其转发的数据包个数.

正常节点有较高的路由转发率和数据转发率, 即满足:

$$\left(R_r \geq R_{r0}\right) and \left(R_d \geq R_{d0}\right) \quad (1)$$

其中, R_{r0} 和 R_{d0} 分别为网络中设置的路由转发率和数据转发率的正常最低阈值, 低于该阈值则认为路由转发和数据转发不正常.

2) 不合作行为

不合作节点是自私节点或者休眠节点, 作为中间节点, 不愿意为其他节点转发路由请求分组和数据分组; 作为目的节点, 正常接收并返回路由应答.

不合作节点的路由转发率和数据转发率很低, 即满足:

$$\left(0 < R_r < R_{r0}\right) and \left(0 < R_d < R_{d0}\right) \quad (2)$$

并且, R_r 和 R_d 更趋向于 0.

3) 恶意攻击行为

恶意攻击行为主要研究了无线自组网中最常见的选择性转发(灰洞)、sinkhole(黑洞)、虫洞、女巫攻击.

① 选择性转发行为(灰洞攻击)

选择性转发一般是恶意节点针对数据包进行的故意丢包行为, 常和其他攻击配合使用. 为了达到吸引数据分组经过的目的, 在路由建立时, 恶意节点并不丢弃路由请求分组, 而是正常配合转发, 仅在建立路由后, 对经过本节点的数据分组选择性丢弃.

选择性转发的路由转发率较高, 数据转发率较低, 即满足:

$$\left(R_r \geq R_{r0}\right) and \left(0 < R_d < R_{d0}\right) \quad (3)$$

② sinkhole(黑洞)攻击行为

Sinkhole 攻击的目的是吸引周围的节点选择它作为路由经过点, 然后和其他攻击(如选择性转发攻击, 篡改报文攻击等)结合起来实施丢包、篡改等攻击. 因此, 它不仅仅是执行路由请求包的转发, 还想方设法让自己成为其他节点的转发节点, 从而吸引数据流经过. Sinkhole 节点在收到路由请求包后, 一方面进行路由转发, 另一方面对收到的每个寻路信息进行回复, 声称自己有一条通向目的节点的高质量路由, 大量发送非正常的路由应答分组. 收到数据包后, 可能选择丢包, 也可能窃听、篡改.

定义 3. 节点物理距离: $d_{ij}=\left|W_i(x,y)-W_j(x,y)\right|$, $W_i(x,y)$为节点 i 的经纬度.

定义 4. 路由应答率: $R_p=\dfrac{n_{pf}}{n_{rr}}$, 其中, n_{pf} 为实际发送的路由应答包个数, n_{rr} 为需要其转发的请求包个数.

定义 5. 数据校验结果: V, 其中, V=0 表示无变化; V=1 表示有变化.

Sinkhole 攻击的路由转发率很高, 路由应答率过多, 与目的节点实际距离远, 数据转发率可高可低. 数据转发率低的话, 就是丢包行为; 如果数据转发率高的话, 可能有信息篡改和窃听行为, 数据校验值变化. 即满足:

$$(R_r \ge R_{r0})and\ (d_{kd} \ge \overline{d}_0)and\ (R_p \ge R_{p0})and\ ((0<R_d<R_{d0})or((R_d \ge R_{d0})and\ (V=1))) \tag{4}$$

其中, $\overline{d}_0$ 为平均单跳距离范围, d_{kd} 为中间节点 K 到目的节点 D 的物理距离, R_{p0} 为正常境况下某节点作为目的节点发送路由应答的比率.

③ 虫洞攻击行为

虫洞攻击的目的也是吸引周围的节点选择它作为路由经过点, 然后和其他攻击结合起来实施丢包、篡改等攻击. 通常是由两个相距较远的恶意节点共谋完成的. 其中一个节点类似sinkhole攻击, 以声称的高质量路由吸引网络数据流, 并发送至共谋节点. 共谋节点间通过一个私有通道(如额外信道、有线连接、包封装等方式)进行通信. 这就造成两个节点为邻居节点的假象, 并被用于之后的路由过程中. 数据在私有通道传输时, 可能遭到窃取、破坏或者篡改.

虫洞攻击与 Sinkhole 攻击的区别在于, 吸引路由的节点并不直接发送应答分组, 而看上去是正常的分组转发, 但是实际上是通过隧道转发给了同谋节点. 因此, 单纯从路由转发率和数据转发率上看, 与正常节点的行为特征相差不大, 即满足:

$$(R_r \ge R_{r0})and(R_d \ge R_{d0}) \tag{5}$$

其中, R_{r0} 和 R_{d0} 分别为网络中设置的路由转发率和数据转发率的正常最低阈值, 低于该阈值则认为路由转发和数据转发不正常. 除此之外, 两个相距较远的两个恶意节点采取某种欺骗或者真实的方式建立一个高速链路时, 还呈现出一些新特征.

目前, 虫洞攻击的实施方法主要有三种. 一是使用额外信道的攻击方式: 两个恶意节点通过一条高带宽的额外信道直接传送路由请求包; 二是高能量传输的攻击方式: 收到路由请求后, 一个拥有高能量的恶意节点以较高的能量广播该请求, 较远的合谋节点收到该路由请求包; 三是使用包封装的攻击方式: 两个恶意节点在传递路由请求包时, 将包封装, 使得跳数计数器在两个恶意节点之间不会增加, 但是实际可能经过很多跳. 不管虫洞攻击采用何种方法实施, 这两个共谋节点肯定不是相邻的, 虫洞攻击中恶意节点声称的距离比实际距离要短. 另外, 虫洞节点一旦成功潜入路由发现后的路径, 就可以吸引大量网络流量, 吞吐量明显加大.

定义 6. 节点发射功率: P_{ri}, 表示节点的物理层发射信号强度.

定义 7. 传帧率: $R_F=\dfrac{n_F}{t}$, n_F 表示 t 时间内发送的数据链路层帧数量.

因此, 虫洞节点的发射功率和传帧率均超过阈值, 并且与邻节点的实际物理距离大于一跳范围, 即还应满足:

$$(P_{ri} \le P_{r0})and(R_F \ge R_{F0})and(d_{kn} \ge \overline{d}_0) \tag{6}$$

其中, P_{r0} 是网络预设的节点最大发射功率, R_{F0} 是节点传帧率最大阈值, d_{kn} 为中间节点 K 到下一跳某个邻节点 N 的物理距离, $\overline{d}_0$ 为平均单跳距离范围.

④ 女巫(sybil)攻击行为

sybil 攻击中, 恶意节点在参与网络通信时, 不断向其他节点声明其多重身份, 节点伪造出来的信息将在网络中的各种路由请求包或者数据包中出现, 建立虚假路由. 事实上, 那些节点都不存在, 所有发往那些节点的数据, 都将被巫师节点获得. 巫师节点收到

数据后, 可以任意窃听、篡改、伪造、丢弃. 但与黑洞节点不同的是, 表面上数据还是经过若干个节点, 而不是集中地流向某个节点.

巫师节点伪造出来的节点可以分为两类: 一类是网络中没有的节点; 另一类是冒充网络中已有的节点. 如果要求所有节点入网时必须登记才合法, 那么伪造的新节点在身份认证时肯定不合格. 如果巫师节点冒充其他节点, 那么它们的物理位置肯定不同. 在正常节点处, 数据转发率何数据校验值肯定是正常的, 没有丢包和篡改行为. 在巫师节点所冒充的节点处, 数据转发率低则是丢包行为; 数据转发率高则可能有信息篡改和窃听行为, 数据校验值变化.

定义 8. 节点 i 身份认证结果: A_i, 其中, A_i=0 表示节点 i 已注册过, 合格; $A_i=1$ 表示节点 i 未注册过, 不合格.

因此, 两个不同物理位置有相同 ID 的节点, 如果身份认证结果、数据转发率、数据校验结果满足以下特征, 则为巫师节点.

$$(A_i=1)or((A_i=0)and((0<R_d<R_{d0})or((R_d\geq R_{d0})and(V=1)))) \tag{7}$$

4) 网络资源耗尽攻击行为

网络资源耗尽表现为大量频繁的分组信道接入和分组发送行为, 主要有反复路由请求、大量路由应答、发送海量无用信息三种.

① 反复路由请求行为

节点作为源节点进行网络资源耗尽攻击, 频繁发送路由请求分组.

定义 9. 路由请求率: $R_q=\frac{n_q}{t}$, n_q 表示 t 时间内发送的路由请求分组的次数.

反复路由请求节点导致传帧率超过阈值, 路由请求率也远远大于正常值, 即满足:

$$(R_F\geq R_{F0})or((R_q>R_{q0})) \tag{8}$$

其中, R_{q0} 为一般正常节点路由请求率的阈值.

② 大量路由应答行为

节点作为目的节点进行网络资源耗尽攻击, 频繁发送大量路由应答分组, 造成网络资源耗用, 还可能传播错误路由信息, 造成网络路由混乱.

大量路由应答行为导致传帧率超过阈值, 路由应答率也远远大于正常值, 即满足:

$$(R_F\geq R_{F0})or((R_p>R_{p0})) \tag{9}$$

③ 发送海量无用信息行为

发送海量无用信息又称直接耗尽攻击. 攻击者针对某个关键节点发送海量的垃圾数据, 占用网络接入资源, 中间节点由于转发这些垃圾数据也将大量消耗电池能量.

定义 10. 发送内容检测结果: C_i, $C_i=0$ 表示节点 i 发送的不是无用信息, 合格; $C_i=1$ 表示节点 i 发送的数据是无用信息, 不合格.

发送海量无用信息的行为特征是:

$$(R_F\geq R_{F0})and(C_i=1) \tag{10}$$

5) 篡改信息攻击

恶意节点篡改信息攻击主要包含两类: 一类是篡改路由信息; 另一类是篡改内容信息.

① 篡改路由信息

篡改路由信息的节点在正确建立路由后, 故意不按照路由列表转发数据, 而是修改转发节点, 导致路由紊乱, 源节点找不到目的节点, 从而不断发起路由请求. 为了避免因恶意节点篡改路由而导致源节点大量发送路由请求造成的节点行为误判, 有必要提取篡改路由信息的节点行为特征.

实施篡改路由信息攻击的节点可能是目的节点, 也可能是中间节点. 如果是目的节点则可能故意不发送路由应答, 发送错误应答, 导致源节点重复路由请求. 如果是中间节点实施攻击, 则是在转发路由应答分组或者转发数据分组的阶段, 篡改源路由列表中的路由信息.

定义 11. 目的节点 m 针对于源节点 n 发送的路由请求是否做出路由应答: L_{mn}, $L_{mn}=0$ 表示做出应答, $L_{mn}=1$ 表示没有做出应答或者应答返回的路由列表错误.

定义 12. 路由列表篡改验证: M, $M=0$ 表示路由列表没有被篡改, $M=1$ 表示路由列表被修改了.

定义 13. 下一跳地址验证: N, $N=0$ 表示实际发送的下一跳地址与路由列表中的下一跳地址一致, $N=1$ 表示实际发送的下一跳地址与路由列表中的下一跳地址不一致.

篡改路由信息的节点行为特征满足:

$$(R_q>R_{q0})and((L_{mn}=1)or(M=1)or(N=1)) \tag{11}$$

② 篡改内容信息

篡改内容信息主要指篡改数据分组的内容信息,

攻击节点在吸引数据分组从自己经过后, 可能不丢包, 只是窃听或者篡改. 可以通过数据加密和数据校验来检验是否有篡改内容信息的行为. 如前面公式 4 所述, 数据校验结果用 V 表示, 当 V=0 时表示无内容篡改行为; 当 V=1 时表示有内容篡改行为.

2　节点行为特征之间的关联关系及检测特征

2.1 检测特征参数

前面, 我们对网络中各类节点的行为特征进行了分析, 发现许多行为有共同之处. 冒充其他节点、sinkhole 攻击、虫洞攻击都存在节点实际位置距离与路由表位置距离不相符的行为; 物理层攻击和虫洞攻击都存在节点发射功率较大的行为; 碰撞攻击、霸占信道、发送海量无用信息等行为均表现为单位时间内接入信道次数较多、传真率高. 因此, 可以用一些典型的行为特征, 作为监测和区分这些攻击行为与正常行为的检测准则.

信息内容完整性、信息内容有用性	应用层
请求转发率、数据转发率、路由请求率、路由应答率、针对性路由应答、路由列表完整性	网络层
传帧率、节点 MAC ID、节点物理位置、下一跳地址正确性	数据链路层
节点信号发射功率	物理层

图 1　多协议层检测特征参数

数据分组和路由请求分组在传输过程中, 在源节点自顶向下从应用层、网络层、数据链路层、物理层逐层封装; 在中间节点, 经物理层、数据链路层的解封, 读取网络层路由信息后, 再封装传输; 到达目的节点后, 自底向上解封读取数据信息内容. 从这一过程来看, 为了检测节点行为类别, 最为方便的顺序是: 物理层、数据链路层、网络层、应用层, 根据每一层的检测特征, 判断其行为类别. 为此, 我们提出了多协议层的检测特征参数.

如图 1 所示, 物理层的检测特征主要: 节点信号发射功率; 数据链路层的检测特征主要是: 传帧率、节点 MAC ID、节点物理位置、下一跳地址正确性; 网络层(路由层)的检测特征主要是: 请求转发率、数据转发率、路由请求率、路由应答率、针对性路由应答、路由列表完整性; 应用层的检测特征主要是: 信息内容完整性、信息内容有用性.

2.2 多种行为类别的关联检测

有些行为必须联合多层检测才能进行正确分类. 如图 2 所示, 我们给出了常见行为类别的分层关联检测流程.

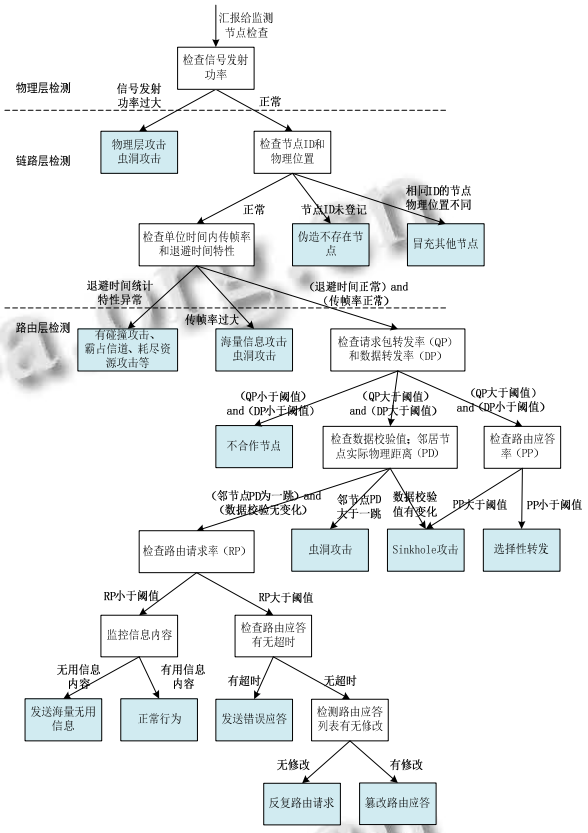

图 2　多种类别节点的关联检测

首先, 根据信号发射功率, 判断节点物理层行为特征, 发射功率明显超出限制范围的节点被认为是不遵守规定、信任度等级较低的节点;

其次, 检查数据链路层的节点 MAC ID、实际 GPS 位置、传帧率, 判断有无网络中没有经过初始注册的节点, 有无 MAC ID 相同但是实际位置不同的冒充节点, 有无长期霸占信道大量发送分组的节点, 这类节点被认为是信任度等级较低的节点.

然后, 检查网络路由层的请求转发率、数据转发率、路由应答率, 判断网络中有无明显不合作转发、应答过于频繁的不正常节点, 降低其信任度等级; 再分别针对源节点检查网络中路由请求率, 针对中间节点检查路由列表完整性、下一跳地址正确性、信息内容完整性, 针对目的节点检查针对性路由应答、信息内容完整性、信息内容有用性, 判断节点的行为类别,

降低其信任等级.

3 行为区分率的仿真分析

为了验证多状态节点行为特征模型的有效性, 我们进行了与能量要素、通信要素的对比仿真实验, 重点研究了网络变化时对正常行为、不合作行为、选择性转发行为、sinkhole 黑洞攻击行为、虫洞攻击行为、女巫攻击行为、反复路由请求行为、大量路由应答行为、发送海量无用信息行为的定级正确率和检测效率性能. 定级正确率是正确划分信任等级节点数与总待测节点的比率. 检测效率包括检测出节点类别需要的因素、步骤和时间, 这关系到检测算法在网络动态变化下的适用性和稳定性.

图 3 为网络中低速变化时基于剩余能量最大、转发率最高和多状态联合检测时, 对各类节点行为定级正确率的比较. 可以看出, 多状态联合检测方法能有效应对网络中大部分的节点恶意行为, 降低节点的信任等级; 能量要素和通信要素则无法有效区分网络中的多种节点行为, 尤其是对于除了选择性转发以外的其它恶意行为的判断能力非常薄弱, 几乎完全是随机的. 这是因为剩余能量和转发率不足以表示节点的行为特征, 反而有些恶意节点为了达到目的会声称自己剩余能量很充足, 并拼命转发吸引网络流量, 造成节点行为定级的错误.

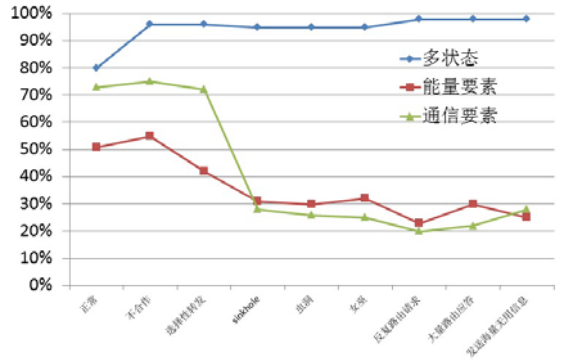

图 3 网络中低速时节点行为的定级正确率比较

图 4 所示为网络拓扑处于不同变化速度时, 节点定级所需的平均时间. 可以看出, 虽然网络拓扑变化加快导致定级时间有所增加, 但是总体定级时间还是比较低的. 在网络变化时, 受变化速度影响较明显的参数主要有传帧率、路由请求率、路由应答率、物理位置, 而警察节点的监测范围较大和监测能力比较强, 并且在平时持续获取检测参数, 当节点移动不至于频繁出入其覆盖范围时, 参数更新不会对定级时间造成非常严重的影响.

图 5 为网络处于静态、中低速变化、中高速变化时各类节点行为的定级正确率. 网络变化增加时, 正常节点行为的定级正确率有显著下降, 其他节点行为虽然也有下降但基本能保持较高水平. 这是因为, 我们的定级机制是发现异常即降低信用度, 只有完全符合正常节点参数特征的才能保持较高信用度. 因此, 虽然网络动态变化时, 虫洞、女巫、反复路由请求行为的检测正确率有所下降, 但是基本不影响对节点异常和降低信用度的判断, 有较好的容错能力. 正常节点则因为涉及的检测参数最多, 判断条件最为苛刻, 检测正确率和定级正确率都有明显降低, 主要体现在将部分正常节点误判为恶意节点, 而降低信用度. 在一定程度上, 可以通过历史信用度的叠加尽量减少误判的影响.

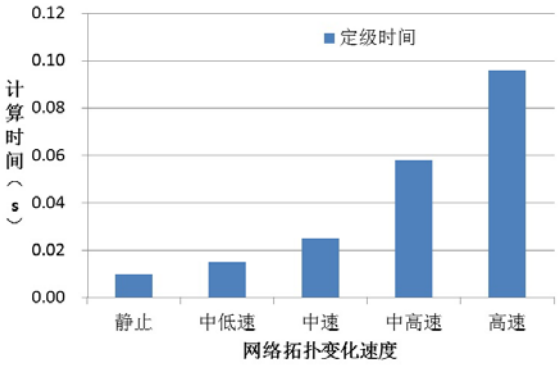

图 4 网络拓扑变化时所需的定级时间

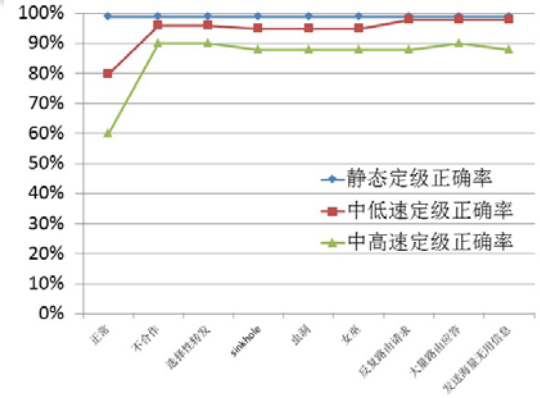

图 5 网络拓扑变化时节点行为的定级正确率

3 结语

节点信任度评估是解决无线自组网安全性问题的

一个有效途径, 其中, 节点行为检测是信任评估模型的重要部分. 从节点行为对网络安全的影响角度看, 节点行为可分为正常、不合作、恶意三类, 而恶意节点将直接导致路由破坏或者毁坏数据. 因此, 在节点行为检测和信任度评估时, 必须首先重点关注其安全性行为特征, 以便降低恶意行为节点的信任值. 本文归纳了网络中九种常见的节点行为类型, 分析了各行为状态的行为特征, 建立了特征模型, 提出了检测特征参数和关联检测模型. 仿真结果表明, 本文提出的节点行为检测特征参数和关联检测模型, 在静态及网络变化时, 对不合作节点、恶意节点的行为信任值评估定级均有较高的准确性, 可以有效地将这些节点排除在网络路由和数据转发活动之外, 有利于网络整体的安全性.

参考文献

1 Boukerche A, Ren Y. A trust-based security system for ubiquitous and pervasive computing environments. Computer Communications, Elsevier, 2008, 31: 4343–4351.

2 Boukerch A. Algorithms and Protocols for Wireless Sensor Networks. Wiley-IEEE Press, ISBN: 978-0-471-79813-2, October 2008.

3 赵曦滨,游之洋,赵志峰.基于 MANET 可用性的信任度量模型.通信学报,2010,31(3):82–88.

4 Abdel-Halim IT, Fahmy HMA, Eldin AMB. Agent-based trusted on-demand routing protocol for mobile Ad-hoc networks. Wireless Networks, 2015,21(2): 467–483.

5 Li X, Jia Z, Zhang P, Zhang R, Wang H. Trust-based on-demand multipath routing in mobile Ad hoc network. IET Information Security, 2010, 4(4): 212–232.

6 Cheng W, Liao X, Shen C, Li S, Peng S. A trust-based routing framework in energy-constrained wireless sensor networks. Wireless Algorithms, Systems, and Applications, 2006: 478–489.

7 Pirzada AA, McDonald C. Establishing trust in pure Ad-hoc networks. 27th Australasian Conference on Computer Science, 2004, 26: 54–63.

8 Li Y, Cong Q, Liu Z, Wang K, Dai B. Ad-hoc multi-dimensional trust evaluation model based on classification of service. 5th International ICST Conference on Communications and Networking in China (CHINACOM), 2010. 1–5.

9 Karthik N, Dhulipala VRS. Trust calculation in wireless sensor networks. 3rd International Conference on Electronics Computer Technology (ICECT). 2011. 376–380.