无线 Mesh 网络中基于复权马尔可夫链的安全路由协议

冯媛媛[1] 易 欣[1] 赵 丽[2]

[1](四川工程职业技术学院电气信息工程系 四川 德阳 618000)

[2](山西大学软件学院 山西 太原 030013)

摘 要 针对无线 Mesh 网络机会路由(OR)机制中的安全性问题:在网络中可能有恶意节点的存在,提出一种基于复权马尔可夫链的安全路由协议。模拟网络中黑洞节点的攻击方式,通过复权马尔可夫链来构建网络中数据转发的线性拓扑模型;通过计算各节点的状态转移概率矩阵来预测丢包率,从而识别恶意节点,并在数据转发过程中避开这些节点。仿真实验中分析恶意节点数量、网络密度和候选集大小对路由协议性能的影响。结果表明,该协议能够识别恶意节点,降低丢包率,提高网络性能。

关键词 无线 Mesh 网络 复权马尔可夫链 节点预测 黑洞攻击 丢包率

中图分类号 TP393 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.07.026

SECURE ROUTING PROTOCOL BASED ON RE-WEIGHTED MARKOV CHAIN IN WIRELESS MESH NETWORKS

Feng Yuanyuan[1] Yi Xin[1] Zhao Li[2]

[1](*Department of Electrical Information Engineering, Sichuan Engineering Technical College, Deyang 618000, Sichuan, China*)

[2](*School of Software, Shanxi University, Taiyuan 030013, Shanxi, China*)

Abstract Aiming at the security problem of opportunistic routing (OR) mechanism in wireless Mesh networks, considering the existence of malicious nodes, we proposed a secure routing protocol based on re-weighted Markov chain. We simulated the attack mode of black hole nodes in the network, and the linear topology model of data forwarding in the network was constructed by re-weighted Markov chain. Then we predicted the packet loss rate by calculating the state transition probability matrix of each node to identify the malicious nodes, and avoided these nodes in the process of data forwarding. In the simulation experiment, we analyzed the influence of the number of malicious nodes, network density and candidate set size on the performance of routing protocols. The results show that the protocol can identify malicious nodes, reduce packet loss rate and improve network performance.

Keywords Wireless mesh network Re-weighted Markov chain Node prediction Black-hole attack Packet loss

0 引 言

机会路由 OR(Opportunistic Routing)[1]算法是一组单播或组播的路由算法,它可以确保无线网络中端到端之间分组路由的可靠性和有效性。与传统的路由方案如 DSV、AODV、OLSR 等[2]不同,OR 算法在路由过程的每一跳中,仅选择一个节点作为下一跳的实际转发器。同时向其传输数据包目的地和相邻节点子集,作为潜在的下一跳转发器。OR 算法中的路由操作分为两个阶段:候选点选择和候选点协调。其中,候选点选择方法近年来受到研究者的高度重视。在候选选择过程中使用不同的度量和参数,例如节点之间的通信链路的质量、节点的地理位置以及潜在候选点的可信度等因素。

科研人员对 OR 中候选节点的选择和协调方法进行了大量研究[3-4]。例如,极端机会路由(ECOR)[5]是一种基于 OR 算法的路由算法,这种路由使用预期

收稿日期:2018-11-19。山西省科技厅基础研究计划项目-青年科技研究基金项目(2014021039-6)。**冯媛媛**,副教授,主研领域:计算机网络,物联网。**易欣**,副教授。**赵丽**,副教授。

传输计数(ETX)作为候选选择的度量。简单机会自适应路由算法(SOAR)[6]同样使用 ETX 指标进行候选选择,源节点和目标节点之间的最短路径使用 ETX 度量来计算,然后通过添加接近最短路径的节点来选择候选集合。最低成本机会路由(LCOR)[7]是另一种 OR 算法,这种路由使用预期任意路径传输(EAX)度量来选择候选节点,该算法能够通过对网络拓扑图进行分析,进而发现最佳候选集合。与 LCOR 类似,文献[8]提出一种代表最小传输选择的 MTS 算法,同样使用 EAX 度量来进行候选点的选择。与这些只考虑候选节点之间链路质量的算法不同,有一类算法考虑了节点的地理位置:文献[9]提出的 DPOR 算法通过考虑每个候选点到目的地的距离来选择候选集;在其改进版本 DPOR[10]算法中,节点之间的链路传递概率和距离组合用于定义候选选择的度量;文献[11]和 DPOR 算法类似,也使用链路质量和节点的地理位置来精确地选择其下一跳转发器。另外,还有一些考虑其他因素的算法。例如,文献[12]提出了一种传输延迟有效的 OR 算法,提高了能量效率;文献[13]在路由数据包传达至目的地的过程中,考虑了服务质量的计算。

目前,大多数研究主要关注可靠性方面,也就是说这些 OR 算法都遵循一个假设,即网络中的所有节点都是良性的协作节点。然而,在实际情况下,网络中可能会出现恶意节点,对无线网络中的通信性能造成破坏性影响。例如,拒绝服务(DoS)攻击[4],其中当恶意节点作为其他节点的下一跳转发器时,这些节点倾向于丢弃所有收到的分组,并降低网络性能。

目前,OR 算法中恶意节点的影响尚未引起足够的重视。因此,本文使用复权马尔可夫链构建一种基于 OR 的无线 Mesh 网络的新模型,用于检测系统中存在的恶意节点,防止其转发数据包。其主要创新点在于:

(1) 采用了一种最新的马尔科夫链技术,即复权马尔可夫链来进行节点预测;

(2) 通过复权马尔可夫链将机会路由中的恶意攻击方式进行建模,通过状态概率的计算来预测恶意节点。

1　路由中的安全问题

除可靠性要求之外,对于安全性的考虑也非常重要。在存在恶意节点的情况下,即使是最可靠的路由算法,在网络中也不能有效的运行。研究表明,采用密码方案是针对恶意节点的一种有效防御机制,它可以保证节点之间数据传输的安全性和完整性。但是,当涉及到逐跳路由中的节点协作时,就可能引入一系列不当行为。例如,一些恶意节点可能会在网络中注入虚假信息,或者阻止节点间的协作。

路由攻击包括黑洞攻击、灰洞攻击和蠕虫攻击。在黑洞攻击(即 DoS 攻击)中,黑洞节点会传输错误的路由信息,试图说服网络中的其他节点选择它们作为路由中的下一跳节点,从而试图吸收尽可能多的数据包,并将它们丢弃。灰洞攻击是黑洞攻击的一个特殊变体。灰洞攻击中,节点倾向于有选择地丢弃一些接收的数据包并转发其他数据包。在蠕虫攻击中,位于不同地区的两个恶意节点相互串连,攻击网络。一旦恶意节点收到一个数据包,就通过一个私有信道把这个包发送到另一个区域,其他恶意节点将在其他区域重发数据包。

为了防御路由攻击,科研人员提出了不同的方法。例如,为了识别网络中不合作的节点,并相应地将其隔离,提出信任和信誉管理协议。文献[14]和文献[15]提出了利用无线网络中节点之间的直接、间接交互构建一些信任和信誉模型。文献[16]则引入机会网络的信任计算方法,接收方节点通过发送正反馈消息(PFM)来确认机会网络中另一个节点的合作性质。

2　复权马尔可夫链

马尔可夫链[17]可以根据事件在以前某个时段的状态转移概率为基础,预测该事件将来的状态变化概率,它主要包括时间参数集 $T=\{0,1,2,\cdots\}$ 和状态参数集 $E=\{0,1,2,\cdots\}$。而在实际应用环境中,常用的是齐次马尔可夫链[18]。假设参数 $u,k\in T$,则:

$$P_{ij}(u;k)\in E \tag{1}$$

式中:$P_{ij}(u;k)$ 表示在 u 时刻,一个随机事件的状态 i 在通过 k 步状态转移计算后变成状态 j 的概率,且该事件的状态 i 发生在 u 时刻。

齐次马尔可夫链在使用过程中将各种状态转移步长看作是同一个值,并不能得到准确的状态预测结果。而复权马尔可夫链对各个步长区别对待,引入权重的概念,将各个状态的预测概率当作权重值,再根据对应的状态均值,实现数值预测。复权马尔可夫链的具体步骤如下:

(1) 创建对象序列的状态分级标准,根据聚类法、频率曲线法等划分不同的状态,并确立对象序列的所属状态。

(2) 对于指标值序列 $x_1,x_2,\cdots,x_n$,当其状态由 i 变为状态 j 时,经历的频数用 f_{ij} 表示,且 $i,j\in E$。然后计算出各个状态的转移规律,从而得出步长的状态转

移频数矩阵。

(3) 转移概率 $P_{ij}(i,j\in E)$ 可以定义为第 i 行第 j 列的元素 f_{ij} 与各行总和的比值,如下式所示:

$$P_{ij}=\frac{f_{ij}}{\sum_{j=1}^{m}f_{ij}} \tag{2}$$

式中:m 表示指标值序列中可能呈现的状态数量,$m\in E$。

(4) 边际概率 $P_{.j}$ 可以定义为 f_{ij} 的第 j 列之和与各行各列的总和的比值,如下式所示:

$$P_{.j}=\frac{\sum_{i=1}^{m}f_{ij}}{\sum_{i=1}^{m}\sum_{j=1}^{m}f_{ij}} \tag{3}$$

统计量 X^2 在序列长度足够大时可表示为:

$$X^2=2\sum_{i=1}^{m}\sum_{j=1}^{m}f_{ij}\left|\lg\frac{p_{ij}}{P_{.j}}\right| \tag{4}$$

根据显著性水平 α 和分位点 $X^2((m-1)^2)$ 的值能够计算出 X^2 的值,当 $X^2>X_\alpha^2\times((m-1)^2)$ 时,该序列可以当作马尔可夫链来处理。

(5) 利用式(5)计算步长的自相关系数:

$$r_k=\sum_{l=1}^{n-k}(x_l-\bar{x})(x_{l+k}-\bar{x})/\sum_{l=1}^{n}(x_l-\bar{x})^2 \tag{5}$$

式中:r_k 表示第 k 个步长的自相关系数,n 表示序列长度,x_l 表示序列的第 l 个值,$\bar{x}$ 表示序列均值。

(6) 根据式(6)将各步长的自相关系数规范化:

$$w_k=|r_k|/\sum_{k=1}^{c}|r_k| \tag{6}$$

式中:w_k 表示规范化后的自相关系数,c 表示最大步长。

(7) 联合转移概率矩阵和初始状态(步长),可以预测出状态概率 P_i^k。

(8) 利用加权算法求和同一状态的不同预测概率,可得该状态的预测概率:

$$P_i=\sum_{k=1}^{m}w_kP_i^k \tag{7}$$

(9) 以 P_i 为权重值,结合相应的 $\bar{x}_i$ 可以得到预测值 z,如下式所示:

$$z=\sum P_i\,\bar{x}_i \tag{8}$$

3 路由中恶意攻击的马尔可夫链模型

OR 方法中的路由操作可以使用复权马尔可夫链进行精确建模,复权马尔可夫链中的每个状态都使用一个元组来定义,该元组包含节点标识符和特定节点中发生的重传次数。文献[19]提出的模型是评估网状网络 OR 性能的一般模型,但这种模型不适用于包含恶意节点的网络。在很多情况下,由于硬件或软件故障等原因,节点并不能像预期的那样参与路由操作。本文提出了一种修改的 OR 算法模型,该模型在网络中含有恶意节点的情况下使用复权马尔可夫链。表 1 为本文所使用的符号和含义。

表 1 符号及其含义

符号	含义
N	网络中的节点数量
M	恶意节点的数量
K	允许的最大重传次数
C	候选节点的最大数量
$\mathrm{CS}_{i,\mathrm{dest}}$	通向目标 dest 的节点 i 的候选集合
S	状态数量
P	转移概率矩阵
Q	瞬时状态之间的转移概率矩阵
R	瞬时状态和吸收状态间的转移概率矩阵
I	吸收状态之间转移概率矩阵
Z	吸收状态和瞬时状态间的转移概率矩阵
V	初始状态
F	复权马尔可夫过程的基本矩阵
ID	节点标识符
$ReTx$	目前为止发生的重传次数
$p_{(i',j')}^{(i,j)}$	状态(i,j)到状态(i',j')之间的转移概率
c_i	第 i 个优先候选节点
$\mathrm{link}_{\mathrm{prob}}(x,y)$	节点 x 和 y 之间的链路传递概率

假设网络中存在 M 个恶意节点,它们都可能执行对应的不合作行为。其中黑洞节点收到数据包后会将其恶意丢弃,但其却宣称转发成功,并向所有其他候选点发送确认消息,指示它已经转发了分组数据。因此,前一跳和所有其他候选点需要阻止这样的分组转发,防止数据包永久丢失。

构建一个 $N=5$、$K=3$、$M=1$ 和 $C=2$ 的线性拓扑结构。在这个模型中,假设所有节点之间的距离相等,并且一个节点(ID = 2)是唯一的恶意黑洞节点,即恶意节点可以收到所有数据包。为此,这样的节点可以模拟为复权马尔可夫链中的吸收状态。更具体地说,一旦系统达到吸收状态,它将保持在该状态,并不再发生状态之间的转换。如图 1 所示,由于 ID = 2 的节点会丢弃对象,因此一旦系统达到状态(2,0),将不能把分组转发到目的地,也不会重传。考虑到这一点,以及

M 个恶意节点的存在,可以计算系统中的状态数量 S:

$$S=(N-M-1)\times(K+1)+M+2 \tag{9}$$

吸收状态的数量将等于 $M+2$,对应于 M 个恶意节点,以及一个失败和一个成功状态。此外,所提出的模型中瞬态的数量为$(N-M-1)\times(K+1)$。一旦复权马尔可夫链中的所有状态都是已知的,就有可能创建一个包含状态间转移概率的随机矩阵。使用该矩阵,可以提取所需的网络参数,例如数据包传输率、丢包率等。

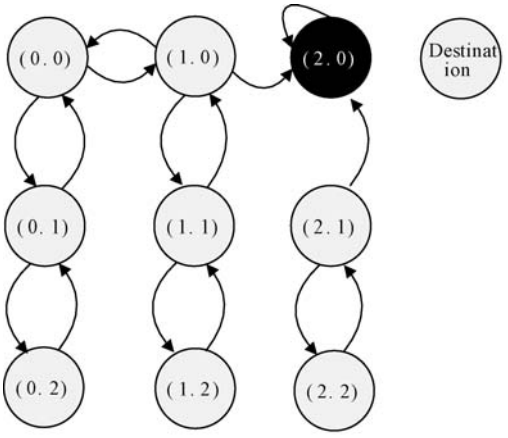

图 1　存在黑洞节点时的线性拓扑模型

转移概率矩阵 $\boldsymbol{P}$ 是一个 $S\times S$ 的矩阵,其表示形式为 $\boldsymbol{P}=\begin{bmatrix}\boldsymbol{Q} & \boldsymbol{R}\\ \boldsymbol{Z} & \boldsymbol{I}\end{bmatrix}$,如图 2 所示。$\boldsymbol{P}$ 由四个不同的子矩阵组成,其中,BH_i 表示第 $i\in M$ 个恶意节点;$\boldsymbol{Q}$ 表示瞬时状态之间的转移概率矩阵,它的维度是$[(N-M-1)\times(K+1),(N-M-1)\times(K+1)]$;$\boldsymbol{R}$ 表示从瞬时状态到吸收状态转移概率的矩阵,它的维度是$[(N-M-1)\times(K+1),(M+2)]$;$\boldsymbol{Z}$ 表示吸收状态和瞬时状态之间的转移概率矩阵,它的维度是$[(M+2),(N-M-1)\times(K+1)]$;$\boldsymbol{I}$ 表示吸收态之间的过渡概率的矩阵,它的维度是$[(M+2),(M+2)]$。

$$\begin{bmatrix} p_{(0,0)}^{(0,0)} & \cdots & p_{(N-M-1,K)}^{(0,0)} \\ p_{(0,0)}^{(1,0)} & \cdots & p_{(N-M-1,K)}^{(1,0)} \\ \vdots & \ddots & \vdots \\ p_{(0,0)}^{(N-M-1,K)} & \cdots & p_{(N-M-1,K)}^{(N-M-1,K)} \end{bmatrix} \quad \begin{bmatrix} p_{BH_1}^{(0,0)} & \cdots & p_{BH_M}^{(0,0)} & p_{Fail}^{(0,0)} & p_{Dest}^{(0,0)} \\ p_{BH_1}^{(1,0)} & \cdots & p_{BH_M}^{(1,0)} & p_{Fail}^{(1,0)} & p_{Dest}^{(0,0)} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ p_{BH_1}^{(N-M-1,K)} & \cdots & p_{BH_M}^{(N-M-1,K)} & p_{Fail}^{(N-M-1,K)} & p_{Dest}^{(N-M-1,K)} \end{bmatrix}$$

$$\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

图 2　转移概率矩阵

当网络中恶意节点的数量较多,特定节点的所有候选都可能成为恶意节点。在这种情况下,由发送节点发送的所有数据包将被候选节点恶意丢弃,即在复权马尔可夫链中数据包成功到达目标节点的可能性为零,即源节点和目的节点之间不存在路径。

4　基于马尔可夫链模型的丢包率预测

4.1　计算转移概率矩阵

一旦知道每个矩阵的维数,就可以计算 $\boldsymbol{P}$ 中每个元素的概率值。如上所述,从状态(i,j)到状态(i',j')的转移概率值定义为 $p_{(i',j')}^{(i,j)}$,其中 i 和 i'表示节点标识符,j 和 j'表示每个节点中发生的重传次数。为了获得概率值,应该考虑不同的情况。另外,所有计算都独立于任何网络拓扑结构,并且对于任何基于 OR 的无线 Mesh 网络都是有效的,和候选节点或重传数量无关。状态的转换概率计算分为以下 4 种情况:

(1) 达到与最高优先级候选节点对应的状态:这种情况说明了将复权马尔可夫链中的一个状态转换到与候选节点集合中具有最高优先级候选所对应的状态的概率。例如,图 2 中的 $p_{(2,0)}^{(0,0)}$ 或 $p_{(3,0)}^{(1,0)}$ 是按照这个规则计算的。这个概率值基本上等于节点 i 和它的最高优先级候选点(如 c_1)之间的链路传递概率:

$$p_{c_1,0}^{i,j}=\mathrm{link}_{\mathrm{prob}}(i,c_1) \tag{10}$$

(2)达到与其他候选对象相对应的状态(除了最高优先级候选节点):在这种情况下,从状态(i,j)转换到状态(i',j')时,i'不是节点 i 的最高优先级候选。此时状态的转换概率可以用下式表示:

$$p_{c_x,0}^{i,j}=\mathrm{link}_{\mathrm{prob}}(i,c_x)\times\prod_{t=1}^{x-1}(1-\mathrm{link}_{\mathrm{prob}}(i,c_t)) \tag{11}$$

(3) 达到重传或失败相对应的状态:如果在传输过程中没有候选点接收到数据包,发送节点倾向于执行重传,最多发生 K 次重传。在这之后,如果没有候选点接收到数据包,则从网络中永久丢弃该节点。计算重传或包传输失败的概率用下式表示:

$$p_{i',j'}^{i,j}=1-\sum_{t=1}^{c}p_{c_t,0}^{i,j} \tag{12}$$

(4) 达到吸收状态:在不同的转换过程中,系统可能达到吸收状态。这种模拟了在 K 次重传之后丢弃分组,成功到达最终目的地的情况,此时状态之间不会发生其他转换,并且系统会创建一个单位矩阵,在转移概率矩阵 $\boldsymbol{P}$ 中表示为 $\boldsymbol{I}$。矩阵 $\boldsymbol{I}$ 通过设置 $p_{i,0}^{i,0}$ 为 1 来创建,其中$(i,0)$表示吸收状态。

4.2　丢包率的计算

通过计算每个与恶意节点相关的从初始状态到达吸收状态的概率,然后将它们组合起来得到丢包率。通过丢包率的预测来判别一个节点是否为恶意节点。

显然,OR 算法中的初始状态与产生数据包的源节点有关。式(13)显示了 OR 的初始状态。从初始状态

V 经过 h 次转换之后到达任意状态的概率可以使用 p^h 来表示,初始状态表示为:

$$V=[1 \quad 0 \quad \cdots \quad 0] \tag{13}$$

本文假设网络中只有一个节点作为源节点,即 ID = 0 节点。这个节点就有必要计算到达与恶意节点相关的每个吸收状态的概率,矩阵 $\boldsymbol{V}\times P^h$ 中的元素 $(0,\mathrm{BH}_i)$ 表示恶意节点 BH_i 接收且丢弃数据包的概率。那么,所有恶意节点丢弃的数据包的总体比率如式(14)所示,其中 M 是恶意节点的数量。由此可以确定达到成功或失败状态的概率,这些值分别代表到达目的地的概率或分组失败的概率。

$$\text{Drop Ratio}=\sum_{i=1}^{M}\mathrm{Drop}_{\mathrm{BH}_i} \tag{14}$$

5 仿真分析

利用 NS 2.35 仿真软件构建仿真环境,分别将本文提出的模型与经典的三种 OR 算法(MTS 算法[8]、POR 算法[9]和 DPOR 算法[10])进行比较。其中,MTS 使用节点之间的链路传递概率来选择候选,其证明了可以根据期望的传输次数(ETX)选择最佳的候选集合。POR 算法则考虑了候选节点的地理位置,为每个节点选择候选集合。DPOR 中候选点的选择不仅考虑了它们的位置,还考虑了链接的质量。

在仿真过程中引入了黑洞攻击,一旦恶意节点接收到分组,就会通知所有其他候选点(以及前一跳节点)它已经接收并转发该分组。其他候选点和前一跳节点会假定该分组已经发送,并且让这些节点放弃发送或重发分组。

5.1 仿真设置

本文使用阴影衰落传播模型进行节点之间的无线通信,参数如表 2 所示。对于单个传输的分组,使用下式计算信号接收到的功率:

$$P_r(d)=10\cdot\log_{10}\left(\frac{P_t\cdot G_t\cdot G_r\cdot\lambda^2}{L\cdot(4\pi)^2\cdot d^{\beta}}\right)+X_{dB} \tag{15}$$

式中:d 表示传播距离,$P_r(d)$ 表示距离 d 处的接收功率,用分贝表示,即单位为 dBW,P_t 表示发射功率,G_t 表示发射天线的增益,G_r 表示接收天线的增益,λ 是信号波长,β 是系统损耗,X_{dB} 代表均值为零、标准偏差为 σ_{dB} 的高斯随机变量。当发送一个数据包时,如果接收节点的接收功率大于或等于一个阈值,比如 RXThresh,节点可以成功接收数据包。因此,可以使用文献[10]中的方式计算在距离 d 处节点 x 和 y 之间的传递概率,如下式所示:

$$\mathrm{link}_{\mathrm{prob}}(x,y)=\mathrm{Probability}(P_r(d)\geqslant 10\log_{10}(\mathrm{RXThresh})) \tag{16}$$

表 2 传播模型参数

参数	值
P_t	0.281 8 W
G_t,G_r,L	1
λ	$\frac{3\times10^8}{914\ \mathrm{MHz}}$
RXThresh	3.652×10^{-10} W
β	2.7
σ_{dB}	6

表 3 列出了仿真研究中使用的所有参数。为深入研究各种参数的影响,选择三个不同的参数进行实验,包括恶意节点数量、节点密度和最大候选数量。所有参数都设置为默认值,然后每次更改一个参数,计算丢包率、数据包传输率和跳数。

表 3 仿真参数

参数	值
传播模型	阴影传播模型
MAC	802.11
节点数	40
网络大小	$500\times500\ \mathrm{m}^2$
恶意节点的数量	6
最多候选节点数	3
最大重传次数	3
数据有效载荷大小	512 比特
传输速率	5 数据包/秒
协调延迟	15 ms
模拟时间	1 800 s

5.2 结果分析

5.2.1 恶意节点数量对性能的影响

本节介绍恶意节点数量对网络丢包率和传输率性能的影响,其中恶意节点的数量从 0 变为 15。由以下仿真结果可知,恶意节点会对网络性能参数产生显着的破坏性影响。

(1) 丢包率。图 3 显示了恶意节点数量对丢包率的影响。丢包率表示为恶意节点丢弃的数据包总数与生成的数据包总数的比例。显然,随着恶意节点数量的增加,丢包率也会随之上升。这是因为当网络中存在更多的恶意节点时,算法中选择这些节点作为候选点的概率增加,因此这些恶意节点有更多机会通过捕获数据分组来攻击网络,并相应地丢弃数据包。

在现有的三种算法中,POR 算法有最低的丢包

率。POR 算法的重点是最小化每个数据包的跳数,这么做降低了恶意节点接收数据包的概率。而在 MTS 算法中,由于整体传输数据包较少,恶意节点捕获数据包的可能性也较小,其丢包率相应较低。而本文提出的算法中丢包率最低,这是因为本文通过复权马尔可夫链来检测恶意节点,能够有效避开恶意节点转发数据,但是当恶意节点数量较多时,会出现不得不通过其转发数据的情况。

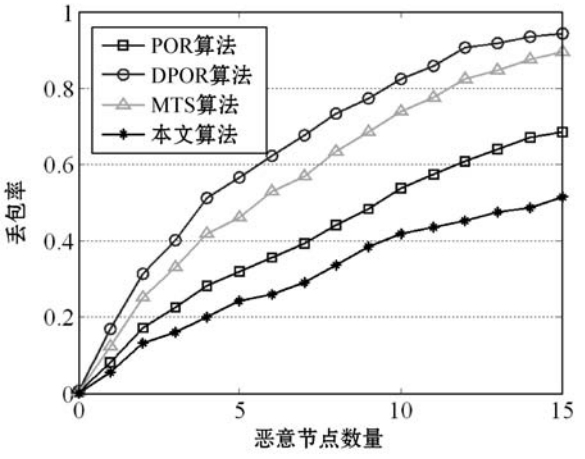

图 3　恶意节点数量对丢包率的影响

(2) 传输率。图 4 显示了恶意节点数量对数据包传输率的影响。传输率是目标节点接收数据包总数与生成的数据包总数的比例。由图 4 可知,增加恶意节点的数量将导致所有算法的传输率下降,因为恶意节点数量的增加将导致捕获和丢弃的数据包数量增加,这显然会导致传输率较低。

在现有的三种算法中,POR 算法的传输率受恶意节点的影响较大,这是因为该算法能够减少在源和目的地之间接收分组的潜在跳数;MTS 算法具有较好的传输率性能。本文算法在传输率方面同样获得了最佳的性能。

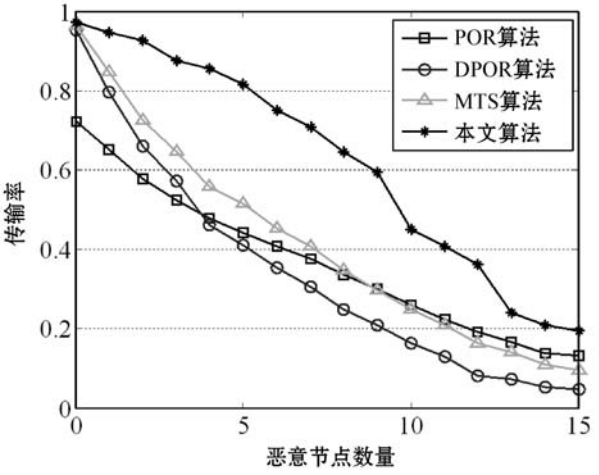

图 4　恶意节点数量对数据包传输率的影响

5.2.2　节点密度对性能的影响

本小节研究节点密度变化对网络性能的影响。对于这种评估,网络尺寸将从 300 × 300 平方米变为 1 000 ×1 000 平方米,而恶意节点的数量都设置为 6 个节点。

(1) 丢包率。图 5 显示了网络大小变化对丢包率的影响。通过扩大网络规模,各种算法的丢包率都是上升到一定水平后开始下降。因为对于较小的网络,例如 300 ×300 平方米,源与目的地之间的路径更短,分组数据需要较少的跳数就能到达目的地。这降低了恶意节点接收数据包的可能性。相比之下,通过扩大网络大小,在路由数据包传递到目的地的过程中涉及到更多的节点,这为恶意节点捕获更多的数据包提供了更多的机会。但是,当网络规模过大时,比如 1 000 ×1 000 平方米,节点之间的平均距离也增大,因此,由于无线信道的阻塞,网络中会有大量的数据包丢失。虽然恶意节点仍然可能被其他节点选为潜在的候选对象,但是只有较少的数据包能够到达目的地。其中,POR 算法性能较好,DPOR 算法性能最差,本文算法同样获得了最佳性能。

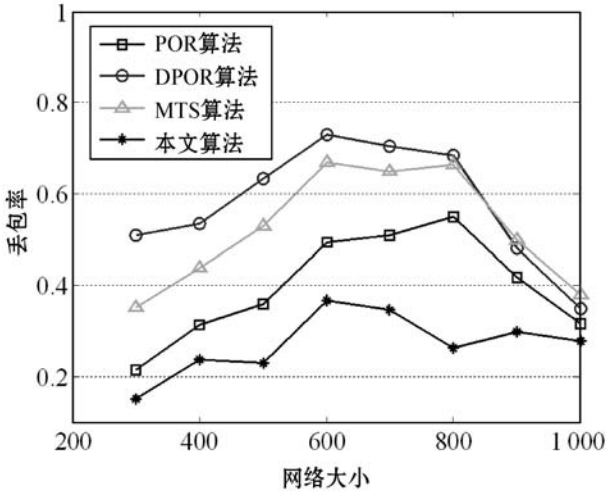

图 5　网络大小对丢包率的影响

(2) 传输率。图 6 显示了网络大小变化对传输率的影响。增加网络规模时,各种算法的传输率都逐渐下降。其原因是恶意节点会捕获和丢弃一些接收到的数据包,并且随着网络规模的扩大,节点之间的距离也越来越大,数据包丢失的可能性也越来越大,因此,更少的数据包将有机会成功传输到目的地。其中,MTS 算法的数据传输性能较佳,DPOR 算法的数据传输性能最差,POR 算法的数据传输性能整体优于 DPOR 算法,这是由于 POR 算法将尝试减少源和目的地之间的跳数,这就使得接收到恶意节点的数据包的可能性减小,传输比率提高。本文算法获得了与 MTS 算法相似

的性能。

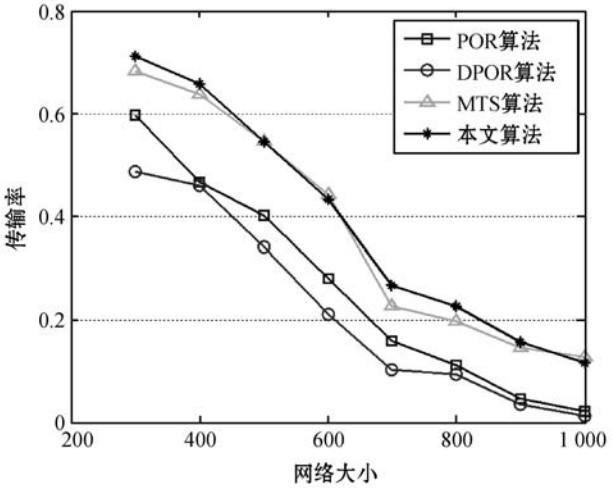

图 6 网络大小对数据包传输率的影响

5.2.3 最大候选节点数量对性能的影响

在这种情况下,候选的最大数目从 1 个节点变为 6 个节点,其他参数则设置为其默认值。

(1) 丢包率。图 7 显示了最大候选节点数量对丢包率的影响。当候选点数目超过 2 个时,DPOR 算法的丢包率变化并不明显,而 POR 算法的丢包率呈现明显上升的趋势,这是因为少数候选点由于传播模型中的分组丢失和能量损失而导致丢失大量分组。事实上,增加候选集中节点的数量会减少数据包丢失的机会,同时增加选择更多恶意候选的可能性。当候选点数量从 1 变化到 3 时,MTS 算法的丢包率呈现略微下降的趋势,当候选节点数量大于 3 时,丢包率几乎不变。与 DPOR 算法相比,MTS 算法中恶意节点可以捕获更少的数据包。本文算法中,能够有效识别恶意节点,所以在候选节点数量变化时,丢包率保持在较低的水平。

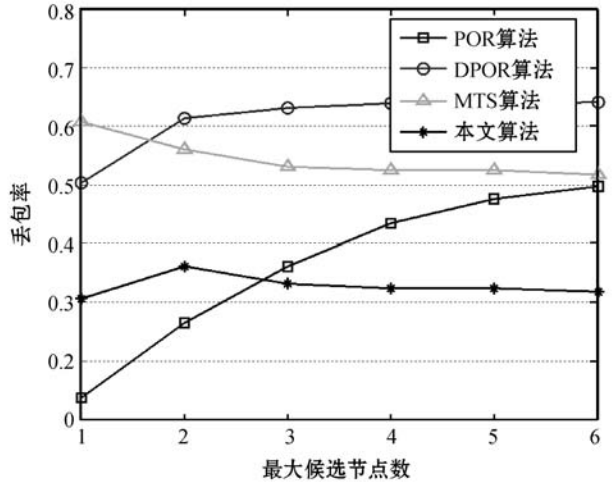

图 7 最大候选节点数量对丢包率的影响

(2) 传输率。图 8 为最大候选节点数量对数据包传输率的影响。在 POR 算法中,随着候选数目的增加,分组丢失的概率减小,而算法尝试通过选择离目的地最近的节点来减少跳数。因此,将数据包发送到目的地的可靠性增加,相应的数据包传输率也增加。当候选集的最大数目少于 3 个节点时,POR 算法表现出较差的传输率。DPOR 算法将地理信息与节点之间的链路传递概率结合起来,具有较好的传输率。当候选点数量从 1 变化到 3 时,POR 和 DPOR 算法的传输率逐渐增加,直到候选点的数量大于 3 个时,传输率趋于稳定。总的来说,MTS 算法在传输率方面的性能较好。由于本文算法受候选节点数量的影响较小,所以传输率也保持在一个较高的水平。

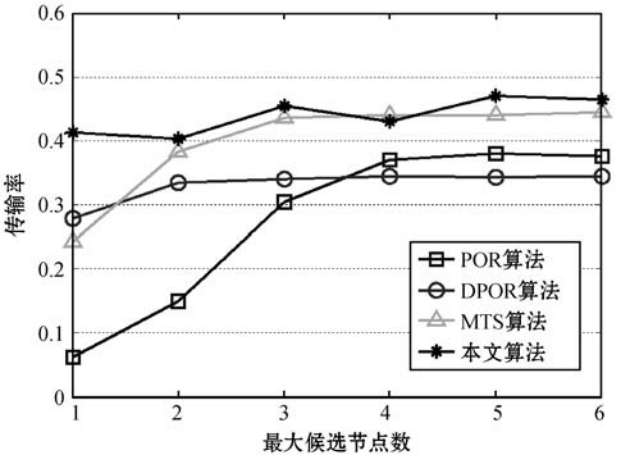

图 8 最大候选节点数量对数据包传输率的影响

6 结 语

本文研究了无线网络中恶意节点对机会路由算法的影响,利用复权马尔可夫链设计并实现了一个新的分析模型来演示恶意节点的存在。另外,为了检测恶意节点,引入了一种计算丢包率的方法。在设计了机会路由算法后,将黑洞攻击作为恶意行为的一个例子,设计并实施了一套综合的性能评估方案,对本文算法和三种经典的机会路由算法进行了仿真分析。结果表明,本文提出的模型能够有效检测恶意节点,提高网络性能。

参 考 文 献

[1] 武淑艳, 韩毅刚, 傅秋宇,等. 基于接触信息的自适应机会网络路由算法中[J]. 计算机应用与软件, 2017, 34(7): 97 - 103.

[2] 沈呈, 陆一飞, 夏勤. 基于综合判据的无线 Mesh 网路由协议[J]. 计算机学报, 2010, 33(12): 2300 - 2311.

[3] Boukerche A, Darehshoorzadeh A. Opportunistic Routing in Wireless Networks: Models, Algorithms, and Classifications [J]. ACM Computing Surveys, 2014, 47(2):1 - 36.

[4] 吴志军, 张景安, 岳猛等. 基于联合特征的 LDoS 攻击检测方法[J]. 通信学报, 2017, 38(5): 19 - 30.
[5] Biswas S, Morris R. ExOR: opportunistic multi-hop routing for wireless networks[J]. Acm Sigcomm Computer Communication Review, 2005, 35(4):133 - 144.
[6] 王博, 黄传河, 杨文忠. 时延容忍网络中基于效用转发的自适应机会路由算法[J]. 通信学报, 2010, 31(10): 36 - 47.
[7] Grossglauser M, Vetterli M. Valuable detours: least-cost anypath routing[M]. IEEE Press, 2011, 19(2): 333 - 346.
[8] Li Y, Chen W, Zhang Z L. Optimal forwarder list selection in opportunistic routing[C]// IEEE, International Conference on Mobile Adhoc and Sensor Systems. IEEE, 2009: 670 - 675.
[9] Yang S, Zhong F, Chai K Y, et al. Position based opportunistic routing for robust data delivery in MANETs[C]//Global Telecommunications Conference,2009. GLOBECOM. IEEE, 2010:1325 - 1330.
[10] Darehshoorzadeh A, Cerdà-Alabern L. Distance Progress Based Opportunistic Routing for wireless mesh networks [C]//Wireless Communications and Mobile Computing Conference. IEEE, 2012:179 - 184.
[11] Salehi M, Boukerche A, Darehshoorzadeh A, et al. Towards a novel trust-based opportunistic routing protocol for wireless networks[J]. Wireless Networks, 2015, 22(3):1 - 17.
[12] Ghadimi E, Landsiedel O, Soldati P, et al. Opportunistic Routing in Low Duty-Cycle Wireless Sensor Networks[J]. Acm Transactions on Sensor Networks, 2014, 10(4): 1 - 39.
[13] Cheng L, Niu J, Cao J, et al. QoS Aware Geographic Opportunistic Routing in Wireless Sensor Networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2014, 25(7):1864 - 1875.
[14] 陈宏亮, 刘莉平, 赵明,等. 认知无线网络中基于信誉度管理的动态频谱接入研究[J]. 计算机工程与科学, 2015, 37(3): 498 - 502.
[15] 肖云鹏, 姚豪豪, 刘宴兵. 一种基于云模型的 WSNs 节点信誉安全方案[J]. 电子学报, 2016, 44(1): 168 - 175.
[16] Li N, Das S K. A trust-based framework for data forwarding in opportunistic networks[J]. Ad Hoc Networks, 2013, 11(4):1497 - 1509.
[17] 李志华, 卢昭, 薛亮,等. 基于马尔可夫链的传感器网络空间相关性数据预测算法[J]. 计算机应用研究, 2016, 33(9): 2747 - 2750.
[18] Loumponias K, Tsaklidis G. Interpretation of the Evolution of the Homogeneous Markov System(or, Equivalently, of the Embedded Markov Chain) as the Deformation of a Viscoelastic Medium. The 3-D Case[J]. Methodology & Computing in Applied Probability, 2017, 19(10): 1 - 13.
[19] Darehshoorzadeh A, Grande R E D, Boukerche A. Toward a Comprehensive Model for Performance Analysis of Opportunistic Routing in Wireless Mesh Networks[J]. IEEE Transactions on Vehicular Technology, 2016, 65(7): 5424 - 5438.

(上接第 147 页)

警等服务,利用无处不在的移动通信网络处理无处不在的无人机,实现全方位的监管。测试结果表明,系统功能基本实现,人机交互友好且稳定性良好,为我国实现对民用无人机的监管提供了一种可实施的方案。

参 考 文 献

[1] Damilano L, Guglieri G, Quagliotti F, et al. Ground control station embedded mission planning for UAS[J]. Journal of Intelligent &Robotic Systems, 2013, 69(1): 241 - 256.
[2] 张建平,任家龙,陈晓. 基于多属性分类的民用无人机空中交通管理模式[J]. 航空计算技术,2017(5):6 - 9,13.
[3] 任丽艳,李英成,薛艳丽,等. 基于北斗技术的无人机飞行监管系统开发与应用[J]. 国土资源遥感,2018(2):238 - 242.
[4] 刘洋,韩泉泉,赵娜. 无人机地面综合监控系统设计与实现[J]. 电子设计工程,2016, 24(14):110 - 112, 115.
[5] 郭杰,王晓银,滑亚慧. 无人机航迹规划与监控系统设计[J]. 计算机测量与控制,2018, 26(9):72 - 77.
[6] Jiang S M, Yao N, Jin X L. Operational conditions of an unmanned aerial vehicle(uav) based underwater data collection system[C]// Proceedings of the 11th ACM International Conference on Underwater Networks Systems. ACM, 2016: 32.
[7] 郑武略,尚涛,张富春,等. 一种低空域的无人机冲突避免系统及方法:中国,201710037737.4[P]. 2017 - 08 - 04.
[8] 赵嶷飞,杨明泽. 基于动作捕捉的无人机运动状态识别[J]. 科学技术与工程,2018, 18(27):53 - 59.
[9] 闫斌,石凯,叶润. 禁飞区无人机预警算法研究[J]. 计算机应用研究,2018(9):2651 - 2658.
[10] 国务院中央军委空中交通管制委员会. 飞行间隔规定[S]. 北京:中国民航出版社, 2003.
[11] Park J, Oh H, Tahk M. UAV collision avoidance based on geometric approach[C]// 2008 SICE Annual Conference, 2008: 2122 - 2126.
[12] Chakravarthy A, Ghose D. Obstacle avoidance in a dynamic environment: a collision cone approach[J]. IEEE Transactions on Systems, Man, and Cybernetics-Part a: Systems and Humans, 1998, 28(5): 562 - 574.