计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(9):241−249 [doi: 10.15888/j.cnki.csa.008684]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

# 基于双层模糊逻辑信任的 OLSR 安全路由协议①

刘　杰, 刘光杰

(南京信息工程大学 电子与信息工程学院, 南京 210044)
通信作者: 刘光杰, E-mail: gjieliu@gmail.com

**摘　要**: 由于移动自组网的开放性、分散性的特点, 导致传统的 OLSR 信任模型存在无法明确量化节点的信任指标和忽视节点的网络环境的问题. 针对上述问题, 本文提出一种基于环境自适应决策的双层模糊逻辑信任模型, 并与 OLSR 协议搭建了 EFT-OLSR 协议. 该模型划分为参数提取模块、双层模糊推理模块、决策模块. 首先选取节点剩余能量 (*P*), 阻止隐式的自私攻击; 其次通过运用改进的双层模糊逻辑结构, 限制计算节点信任指标的复杂度; 最后根据网络环境动态调整路由协议中的信任阈值. 实验表明, EFT-OLSR 协议在数据包传递率 (PDR)、平均端到端延迟、丢包率方面优于现有的 FT-OLSR 信任模型.

**关键词**: 模糊逻辑; 自适应阈值; 多属性准则; OLSR 协议

引用格式: 刘杰,刘光杰.基于双层模糊逻辑信任的 OLSR 安全路由协议.计算机系统应用,2022,31(9):241–249. http://www.c-s-a.org.cn/1003-3254/8684.html

## Secure OLSR Routing Protocol Based on Two-layer Fuzzy Logic Trust Model

LIU Jie, LIU Guang-Jie

(School of Electronics and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China)

**Abstract**: Due to the open and decentralized characteristics of mobile ad hoc networks, the traditional optimized link state routing (OLSR) trust model cannot clearly quantify the trust indexes of nodes and ignores the network environments of nodes. To solve the above problems, this study proposes a two-layer fuzzy logic trust model based on environment-adaptive decision-making and constructs an EFT-OLSR protocol with the OLSR protocol. The model is divided into a parameter extraction module, a two-layer fuzzy reasoning module, and a decision-making module. To start with, the node residual energy (*P*) is selected to prevent implicit selfish attacks; then, the complexity of the trust indexes of the computing nodes is limited by using the improved two-layer fuzzy logic structure; finally, the trust threshold in the routing protocol is dynamically adjusted according to the network environment. Experiments show that the EFT-OLSR protocol is superior to the existing FT-OLSR trust model in packet delivery rate (PDR), average end-to-end delay, and packet loss rate.

**Key words**: fuzzy logic; adaptive threshold; multi-attribute criterion; optimized link state routing (OLSR) protocol

## 1　引言

MANET 是一种自组织网络, 移动节点通过无线链路和多跳转发连接, 没有固定的网络基础设施[1]. MANET 由于其灵活性强, 广泛应用于救灾、车载网络、军事服务等领域. 然而, 由于其分布式特性、网络拓扑结构的不断动态变化和没有绝对控制中心, MANET 容易受到恶意节点的各种攻击[2].

MANET 中的通信分为两种类型: “单跳通信” 和 “多跳通信”. 在前者中, 位于彼此通信范围内的节点直接通信, 而在多跳通信中, 当目的节点超出源节点通信

① 收稿时间: 2021-12-19; 修改时间: 2022-01-18; 采用时间: 2022-01-26; csa 在线出版时间: 2022-06-24



© 中国科学院软件研究所 http://www.c-s-a.org.cn

范围时, 需要中间节点将消息中继到目的节点. 从广义上讲, 路由协议可以分为 3 类: 主动路由协议、被动路由协议、混合协议[3]. 在主动路由协议中, 仅当需要将数据包发送到特定目的地, 并且没有可用的缓存路由时, 才会获得路由. 如动态源路由 (dynamic source routing, DSR)、即按需距离矢量路由协议 (ad hoc on-demand distance vector routing, AODV). 在被动路由协议中, 所有的路由都是预先发现的, 所有的路由都是可用的, 并且一直由网络中的所有节点维护. 如目的节点序列距离矢量 (destination sequenced distance vector, DSDV) 路由协议、优化状态链路路由协议 (optimized link-state routing, OLSR)[4]. 在混合协议中, 这类协议是主动和被动协议的混合. 对于本地邻居, 使用主动技术, 对于较远的节点, 使用被动路由机制. 区域路由协议 (zone routing protocol, ZRP) 是一种混合路由协议. 目前 MANET 常用的路由协议之一是 OLSR, 该协议是对传统路由协议链路状态的改进, 使用了多点中继 (multi-point relay, MPR) 技术[4], 每个节点在其所有单跳邻居之间最优选择一个 MPR 的子集, 以覆盖所有的 2 跳邻居, 且只允许 MPR 节点生成和转发 (topology control, TC) 广播消息, 大大减少了网络中的中继数量和信息量. 但 OLSR 与传统路由协议相比, 需要大量的带宽和能源资源、开销, 且不支持多播和安全性. 因此, OLSR 容易遭受各种恶意攻击, 如黑洞攻击、重放攻击、自私行为等[5]. 黑洞攻击最具破坏性, 攻击者通过谎称到达目的地的最短路径来吸引所有数据包, 后将数据全部转储, 恶意阻止数据转发到目的节点. 此外, 恶意节点渗透到网络中, 会修改、盗用、注入数据, 甚至产生虚假消息. 攻击会采取“自私”的形式[6], 当一个或多个节点拒绝将流量中继到网络的其余节点时, 为了保留能量, 攻击者会隐式地阻止节点之间的通信.

当前增强 OLSR 安全性的工作主要基于密码学方法. Semchedine 等人[7] 提出了一种对标准 OLSR 路由协议的扩展, 称为加密优化链路状态路由 (CRY OLSR), 以保护其免受黑洞攻击. 该提议的机制基于非对称密码, 允许识别并隔离网络中的恶意节点, 但基于非对称加密算法的现代密码学通常是沉重的, 计算压力和能耗高. Baadache 等人[8] 提出了一种基于认证的端到端确认的方法, 用来检查中间节点对数据包的正确转发, 可检测出自组网络中的黑洞攻击. 该方案的局限性是可以防止外部攻击, 但仍然容易受到内部攻击. 综合来说, 基于密码学的安全路由协议由于需要额外的信息交换, 网络和计算开销大, 以及密钥管理和公钥基础设施的支持, 对资源有限的移动设备不友好, 且无法应对存在内部恶意节点的攻击场景.

基于信任模型的安全路由设计总体轻量却能较好应对内部攻击场景, 已受到了广泛关注. 如 Shcherba 等人[9] 提出了一个新的布尔值信誉模型, 该框架由 3 个模块 (信誉模块、信任模块和加权模块) 组成, 并与 OLSR 路由协议交互以减轻丢包攻击. 每个节点的信誉模块计算所有其他节点的本地信誉值, 并将这些值收集在网络中广播的信誉向量中. Bhuvaneswari 等人[10] 提出利用虚构节点检测和防止网络中导致虫洞、黑洞以及灰洞攻击. 这些恶意入侵者通过虚假 HELLO 消息和基于虚拟节点定期发送的 TC 消息验证被及时识别. 尽管已经提出了许多信任管理方案来评估信任值, 但是没有一项工作明确地说明应测量什么来评估网络信任. 在此基础上, Tu 等人[11] 提出了建立基于云模型和模糊 Petri 网的 CFPN 信任推理机制来计算节点的信任值, 通过设置固定的阈值检测[12] 和排除恶意节点. 该方法由于网络传输范围短、节点移动性高, 在网络拓扑频繁变化情况下设置一个固定的信任阈值, 将很难权衡误报率、检测率、丢包率等性能指标[13]. Inedjaren 等人[14] 利用模糊逻辑模型, 将模糊的、随机的节点可信度的性能指标由定性描述转化为定量描述, 评估网络信任和减少计算开销. 该方案中节点的信任值是基于单个信任属性标准来计算的, 可能会出现自举时间问题[15], 即基于信任的方案在网络中建立信任所需的时间, 将会给恶意节点提供更多的机会来丢弃数据包并在网络中长时间不被发现, 且静态阈值的设置难以适应网络环境的动态性.

为解决上述问题, 本文提出一种基于环境自适应决策的双层模糊逻辑信任 OLSR (EFT-OLSR) 作为原始 OLSR 的安全扩展协议. 该模型使用双层模糊逻辑计算节点的信任级别, 极大降低计算的复杂度; 并根据链路变化率、节点度、2 跳连通性动态调整信任阈值, 隔离恶意节点, 有效检测恶意节点发起的黑洞攻击和自私攻击.

## 2 基于环境自适应决策的双层模糊逻辑信任路由 (EFT-OLSR) 协议

OLSR 协议是典型的先验式链路状态协议, 也是



© 中国科学院软件研究所 http://www.c-s-a.org.cn

802.11s 推荐的无线 Mesh 网路由协议[16]. 该协议主要采用两个路由消息: 握手 (HELLO) 和拓扑控制 (TC) 消息, HELLO 消息用来执行链路感知, 邻居检测和 MPR 选择, TC 消息用来声明 MPR 信息. 其次, 该协议引入了多点中继 (MPR) 节点的概念, MPR节点周期性发送 TC 消息, 将拓扑信息扩散到整个网络. OLSR 协议具有以下两个优点:

1) 只有 MPR 节点才能转发 TC 消息, 减小了路由发现过程中洪泛消息的数量.

2) 节点发送的 TC 消息, 只包括与多点中继选择者节点 (MPR selector) 之间的链路信息, 减小了路由发现过程中洪泛消息的长度.

一个节点想要将数据包发送到目的节点, 首先需要将这个包发送到它的 MPR 节点, 所以 MPR 节点是攻击者的中心目标. 为了检测和防止恶意节点发起的黑洞攻击和自私攻击, 本文提出一种基于环境自适应决策的双层模糊逻辑模型, 将该模型嵌入到 OLSR 协议中, 首先通过模糊逻辑计算所属节点的可信度水平; 其次根据网络环境中链路变化率、节点度、2 跳连通性, 构建出动态的信任阈值. 当一个节点的可信值小于阈值时, 该节点就被标记为恶意节点, 避免了恶意节点作为 MPR 节点, 有效的解决了黑洞攻击和自私攻击, 提高网络性能. 其模型框架如图 1 所示.

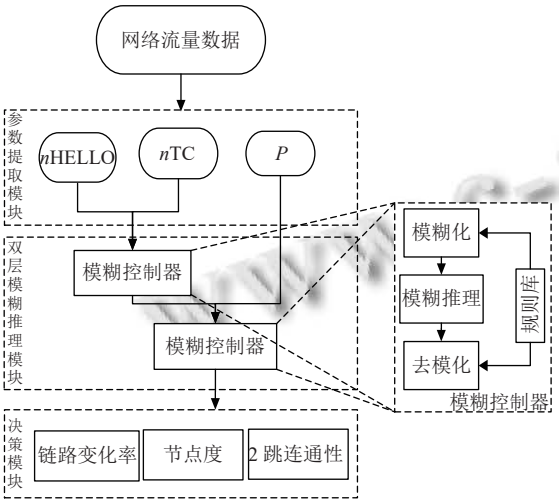



图 1 模型框架

### 2.1 参数提取模块

基于信任路由机制的方案中, 参数提取往往基于单一的属性标准[16]. 如 FT-OLSR 中仅选取数据包数量属性进行决策, 未考虑到节点因自私攻击, 造成的数据包大量丢失. 由于节点频繁的加入和离开网络, 使用单一的属性准则会花费更多的时间去建立信任模型, 给行为不端的节点提供更多的机会破坏网络的拓扑结构, 最终不能有效的发现并处理恶意节点. 为了加快信任机制的建立过程, 有效的处理恶意节点行为, 在参数提取时, 采用多个属性的标准. 于是选取数据包数量属性和节点的剩余能量属性, 避免一个或多个节点拒绝将流量中继到网络的其余节点的情况, 而造成的自私攻击.

1) HELLO 消息的数量和 TC 消息的数量 (*n*HELLO, *n*TC)

在 OLSR 中, 最主要的两个属性是 HELLO 消息和 TC 消息. HELLO 消息用来执行链路感知, 邻居检测和 MPR 选择, TC 消息用来声明 MPR 信息. 因此, 在参数提取时要考虑节点产生的 *n*HELLO 和 *n*TC.

2) 节点剩余能量 (*P*)

由于节点的频繁移动会消耗大量的能量, 有些节点为了保护自身的能量消耗, 会采取“自私”的攻击形式, 隐式地阻止节点之间的通信. 这种恶意攻击常常难以被发现. 在资源受到限制的情况下, 参数提取时必须考虑到节点的剩余能量[15].

### 2.2 双层模糊推理模块

FT-OLSR 中选取两输入单输出的 Mamdani[17] 进行决策, 其模糊规则数增加为指数级, 在资源有限的移动设备中实现该构造会增加计算负载和路由开销. 本文通过运用双层模糊逻辑结构, 使得模糊规则数极大减少, 限制了计算的复杂性, 加快模糊控制器的响应速度, 如图 2 所示.

在第一层模糊结构中, 选取那些对输出结果有着较大影响的变量为第一层结构的输入变量, 即 *n*HELLO 和 *n*TC; 接着选取对输出结果有着次要影响的变量: 节点剩余能量 (*P*), 与第一层结构的输出变量 *M* 共同作为第二层结构的输入, 其结构图如图 3 所示.

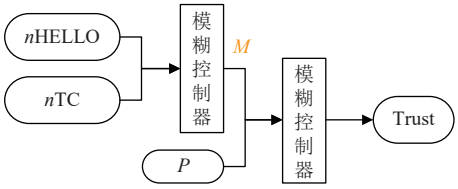



图 2 双层模糊逻辑结构

1) 模糊化处理

计算信任值检查节点的行为, 即“正常或恶意”, 其



© 中国科学院软件研究所 http://www.c-s-a.org.cn

基础是 TC 信息的数量和 HELLO 信息的数量. 因此, 把这两个变量作为模糊系统第一层的输入, 对每个输入使用两个隶属度级别: 低、高. 通过使用相应的预定义变量和隶属函数[18], 将 *n*HELLO 和 *n*TC 化为模糊语言变量. 如图 3 所示, HELLO 隶属函数的数量估计了 *n*HELLO 值的程度. *n*TC 的隶属函数也定义在图 3 中.

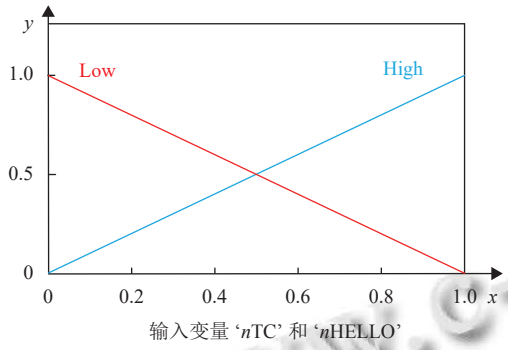



图 3 *n*HELLO 和 *n*TC 的隶属函数

第 1 层结构有一个输出变量: *M*, 同时与节点剩余能量 (*P*) 共同作为第 2 层结构的输入变量, 其模糊语言变量可被定义为: {Low, Medium, High}, 其隶属度函数表示如图 4 所示.

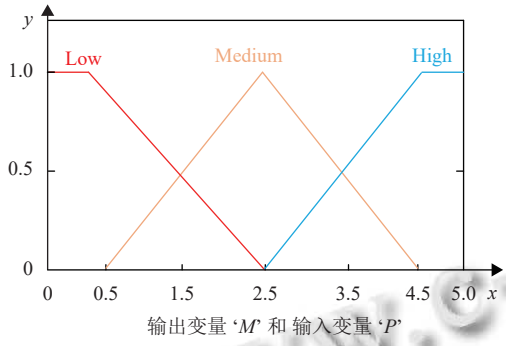



图 4 *M* 和 *P* 的隶属函数

第 2 层结构的输出为: Trust, 也是整个模糊系统的输出. 模糊语言变量可被定义为: {Very low, Low, Medium, High, Very high}, 其隶属度函数如图 5 所示.

2) 模糊规则库的构建

在该模型中, 为模糊推理模块[19] 建立了一个规则库. 采用了 If-then 规则, 则第一层的模糊规则可表示为:

If (*n*TC is $N_i$ and *n*HELLO is $N_i$) then (*M* is $M_m$)

$$N \in \{\text{Low}, \text{High}\}; M \in \{\text{Low}, \text{Medium}, \text{High}\}$$

$$i = j \in \{1,2\}; r_0 \tag{1}$$

第 2 层的模糊规则可表示为:

If (*M* is $M_i$ and *P* is $P_i$) then (*Trust* is $T_m$)

$$Trust \in \{\text{Very low}, \text{Low}, \text{Medium}, \text{High}, \text{Very high}\}$$

$$i = j \in \{1,2,3\}; m \in \{1,2,3,4,5\} \tag{2}$$

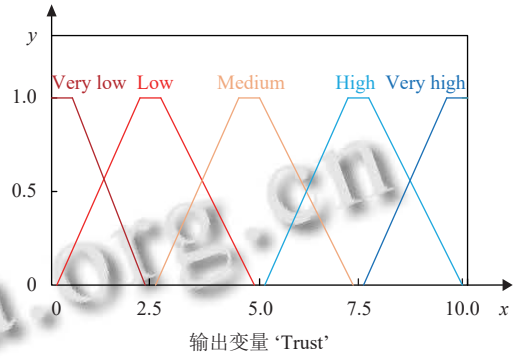



图 5 Trust 的隶属函数

3) 去模化

该模型采用加权平均法进行去模化处理, 并利用式 (3) 对节点的信任值进行预测:

$$Trust(x) = \frac{0.2\times VL(x)+0.4\times L(x)+0.5\times M(x)+0.6\times H(x)+0.9\times VH(x)}{VL(x)+L(x)+M(x)+H(x)+VH(x)} \tag{3}$$

$VL(x)$: 1 跳邻居节点 $x$ 的信任度, 对应信任度为 Very low.

$L(x)$: 1 跳邻居节点 $x$ 的信任度, 对应信任度为 Low.

$M(x)$: 1 跳邻居节点 $x$ 的信任度, 对应信任度为 Medium.

$H(x)$: 1 跳邻居节点 $x$ 的信任度, 对应信任度为 High.

$VH(x)$: 1 跳邻居节点 $x$ 的信任度, 对应信任度为 Very high.

信任值介于 0 到 1 之间. 当信任水平值较低时, 节点表现出的恶意行为多于相邻节点的正常行为.

### 2.3 决策模块

由于 MANET 中的节点具有移动性, 网络拓扑变化频繁, 因此, 很难在基于信任的方案中设置一个合适的信任阈值, 检测出恶意节点. FT-OLSR 中仅使用静态的、预定义的信任阈值, 忽视每个节点的网络环境. 使用静态阈值会导致高误报率和低恶意节点检测率. 若阈值太低, 错误率将会很高, 从路由路径中移除恶意节点会迟缓. 为解决上述问题, 在该模块中, 采用了一种新的环境自适应的决策方法, 该策略根据网络条件调整路由协议中的信任阈值.



© 中国科学院软件研究所 http://www.c-s-a.org.cn

2.3.1 网络模型

本文考虑由一些移动节点组成的自组网. 设该网络模型为图$G(V,E)$, 其中 $V$ 是节点的集合, $E$ 是链路的集合[20]. 所有节点都有一个均匀的传输范围$r_0$, 当且仅当节点 $x$ 与 $v$ 之间的欧氏距离小于传输范围$r_0$时, 无线链路$(x,v)\in E$.

2.3.2 网络参数

1) 链路变化率($\eta$)

由于网络的移动性, 网络的组成以及各个节点的邻域经常发生变化. 节点可通过计算邻域链路变化的速率来确定其邻域内节点的可移动性. 设 $x$ 是一个节点, 关注单个节点 $x$ 的链路变化率[21], 从而得到节点 $x$ 平均的链路变化率为:

$$\eta_x=\lambda_x+\mu_x \tag{4}$$

其中, $\lambda$表示平均链路连接率, $\mu$表示平均断链率, $\eta$表示平均链路变化率.

每一个新节点进入节点 $x$ 的传输范围, 就会产生一条到 $x$ 的新链路, 因此 $x$ 附近的新节点数等于每一个时间间隔 $[t-1,t]$ 下在 $x$ 处的链路连接率, 设为$\lambda_x$:

$$\lambda_x(t)=\{v\in V_x, D_{E(t-1)}(x,v)>r_0\wedge D_{E(t)}(x,v)\leqslant r_0\} \tag{5}$$

同理, 断链数为每个时间间隔 $[t-1,t]$ 内移动出节点 $x$ 传输区域的节点总数. 断链率设为$\mu_x$:

$$\mu_x(t)=\{v\in V_x, D_{E(t-1)}(x,v)\leqslant r_0\wedge D_{E(t)}(x,v)>r_0\} \tag{6}$$

节点 $x$ 在 $t$ 时刻的最小链路变化率为 0, 表示没有新的节点到达, 也由于没有移动的节点而导致的链路中断 (网络是临时静态的). 同样的, 当节点 $x$ 在 $t$ 时刻, 所有与其直接相连的邻居都不在传播范围, 则可能出现最大断链率. Samar 等人[22] 表明, 当最大的链接连接率等于断链率时, 最大链路变化率可为:

$$\lambda_x\max(t)+\mu_x\max(t)=2\times\sigma_x(t) \tag{7}$$

若邻域的链路变化率较高, 考虑到节点间交互时间较短, 较低的信任阈值可能是避免误报的最佳选择. 同样, 如果一个邻域内的链路变化率较低, 则网络趋向于静态, 因此较高的信任阈值可能是最佳选择. 对于链路变化率, 其最优的信任阀值公式如下:

$$\xi_\eta(t)=1-\frac{\eta_u(t)}{2\times\mu(t)} \tag{8}$$

2) 节点度($\ell$)

定义为一个节点的 1 跳邻居中的节点数量. 设 $x$ 为节点, $x$ 在 $t$ 时刻的节点度定为$\ell_x(t)$, 传输范围为$r_0$定义为:

$$\left|\{v\in V_x: D_{E(t)}(x,v)\leqslant r_0\right| \tag{9}$$

节点度为 0 的节点是孤立的, 即没有邻居; 因此, 最小节点度$\min(\ell_x)=0$. 此外, 如果网络中所有节点都直接连接到 $x$, 则节点有最大节点度$\max(\ell_x)$, 节点度直接影响信任阈值. 在计算信任阈值时, 每个节点都考虑其 1 跳邻域内的节点度. 1 跳邻居的节点度越高, 信任阈值越高, 反之亦然. 当源节点有更多可供选择的 1 跳节点时, 可以容忍更严格的信任阈值, 网络分区的风险也更低. 如果将恶意的节点 $m$ 与路由路径隔离, 节点 $x$ 仍然可以连接到网络中. 通过式 (10), 可以找到节点 $x$ 处的最优信任阈值:

$$\xi_\ell=\frac{\ell_x}{V} \tag{10}$$

由式 (10) 可知, 节点度的最大值为最高信任阈值 (1), 节点度的最小值为最低信任阈值 (0).

3) 2 跳连通性

设仅通过邻居 $z$ 可达的 2 跳邻居的节点数 $w$, 则节点 $x$ 的 2 跳邻居定义为:

$$2hop(x)=\{w\in V, z\in V:(x,z)\in E\wedge(z,w)\in E\} \tag{11}$$

节点 $x$ 的 2 跳连通性$\sigma(x,z)$定义如下:

$$\sigma(x,z)=\{W\in 2hop(x):(x,z)\in E_x\wedge(z,W)\in E_x)\} \tag{12}$$

对于特定的 1 跳邻居 $z$, 节点$\min(\sigma_x)$最小 2 跳连通性为 0, 表明通过该节点不能达到任何 2 跳节点. 相反, 一个节点其邻居 $z$ 的最大 2 跳连通性最大值是$|2hop(x)|$, 这表明 $x$ 的所有 2 跳邻居只能通过节点 $z$ 到达.

2 跳连通性是一个重要参数, 表示网络对节点故障的容忍度, 将行为不正常的节点与路由路径隔离之前, 确保网络的连通性. 其 2 跳连通性$\sigma(x,z)$的最优信任阈值公式如下:

$$\xi_\sigma=1-\frac{\sigma(x,z)}{|2hop(x)|} \tag{13}$$

由式 (13) 可知, 当$\sigma(x,z)$值最大时, 信任阈值最小 (0), 当$\sigma(x,z)$值最小时, 信任阈值最大 (1).

将以上的方程合并到数学模型中, 计算恶意节点的信任阈值为:

$$\xi_x=\frac{\xi_\ell+\xi_\sigma+\xi_\eta}{3} \tag{14}$$

最后为了保持高保真的仿真场景, 需将式 (14) 计



© 中国科学院软件研究所 http://www.c-s-a.org.cn

算的信任阈值作为性能指标测试的依据.

### 2.4 EFT-OLSR 协议

EFT-OLSR 路由协议的主要模块是信任管理机制. EFT-OLSR 路由协议以上述提出的多属性环境自适应决策的模糊逻辑信任模型为基础, 这些组件之间关系如图 6 所示.

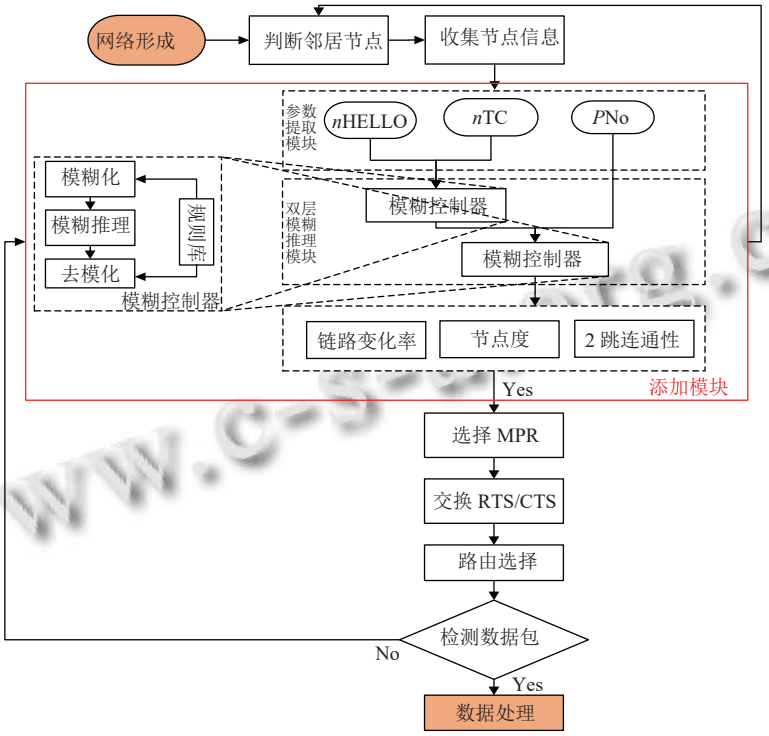



图 6 EFT-OLSR 协议流程图

## 3 仿真实验与分析

该实验采用网络模拟器 3 (NS-3) 进行了测试该方案的性能. 为了获得可靠的结果, 要确保部署的仿真场景能够高保真地表示所提出方案.

### 3.1 仿真环境构建

为实现这一目标, 考虑了网络节点的随机部署, 以更好地评估提出的方案. 在仿真实验中, 将节点的移动速度在 1–10 m/s 之间变化. 并且节点移动性采用 Constant Waypoint mobility model 移动性模型; 且随机选择恶意节点, 以保持其在网络中的分布均匀. 恶意节点数设置为节点总数的 10%–60%. 在实验中, 让恶意节点以 25% 的概率随机或有选择地丢弃数据包来模拟这种攻击. 与真实场景中一样, 恶意节点与常规节点没有区别, 因此具有相同的移动属性, 如速度、方向等. 模拟场景的参数如表 1 所示.

### 3.2 性能指标

仿真中, 通过不同的性能指标测试设计方案, 以下为分析提出的方案时考虑的性能指标:

1) 数据包传递率 (PDR): 源节点产生的数据包数量与目的地接收到的数据包数量的比率.

2) 平均端到端延迟: 数据包从源节点发送到目的地所花费的平均时间.

3) 丢包率: 行为不正常的节点丢失的数据包占发送数据包总数的百分比.

表 1 模拟场景的参数

| 参数 | 值 |
|---|---|
| 节点数 | 50 |
| 仿真时间 | 100 s |
| WiFi 模型 | ad hoc |
| WiFi 速率 | 2 MB |
| 移动模型 | Constant Waypoint mobility model |
| 使用协议 | OLSR |
| 网络规模 | 1000 m×1000 m |

### 3.3 模拟结果与分析

测试 1: 不同节点速度下的性能比较.

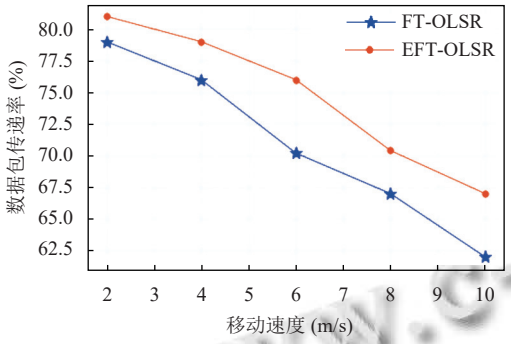
1) 数据包传递率 (PDR)

该测试比较不同节点速度下 FT-OLSR 和 EFT-

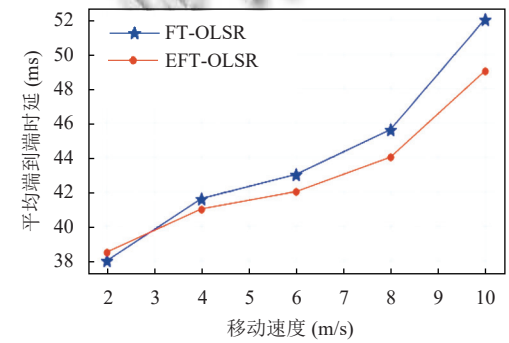


© 中国科学院软件研究所 http://www.c-s-a.org.cn

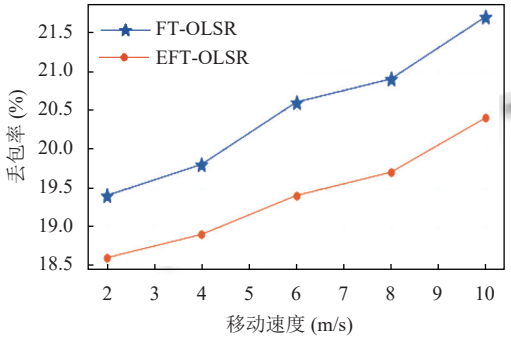
OLSR 性能. 图 7(a) 表明, 两种路由协议的 PDR 都随着节点移动速度的增加而降低. 在较低的节点速度下, EFT-OLSR 比 FT-OLSR 性能更好, 因为链路变化速率越低, 自适应阈值越严格, 恶意节点在较早期就被隔离, 并保持较高的数据包传递率. 然而, 随着节点速度增大, 链路变化速率较高, 自适应阈值保持较低水准, 导致 EFT-OLSR 的数据包传递率较低, 但仍高于 FT-OLSR.




(a) 数据包传递率




(b) 平均端到端时延




(c) 丢包率

图 7 不同节点速度下的性能比较

2) 平均端到端延迟

如图 7(b) 所示, 两种协议的平均端到端延迟都随着节点速度的增加而增加, 随着节点速度的提高, 链路连接很容易崩溃. 因此, 源节点在发送包之前必须发起更多路由请求, 这增加了这两种协议的平均端到端延迟. 相对于 FT-OLSR 协议, EFT-OLSR 的平均端到端延迟相对较高. 因为为了保证较高的数据包传递率, 可能会使数据包沿较长的路径行进, 以避免恶意节点的出现.

3) 丢包率

如图 7(c) 所示, 两种协议的丢包率都随着节点速度的增加而增加, FT-OLSR 的丢包率显著上升, EFT-OLSR 的丢包率缓慢上升. 这是因为 EFT-OLSR 用较高的时延, 保证了较高的数据包传递率, 防止恶意节点转发数据包. 然而, FT-OLSR 没有考虑网络拓扑的变化, 未能有效阻止恶意节点, 导致恶意节点随机的丢弃数据包, 造成丢包率大幅度上升.

测试 2: 不同恶意节点数量的性能比较

1) 数据包传递率 (PDR)

图 8(a) 显示了在改变恶意节点数量时 FT-OLSR 和 EFT-OLSR 的 PDR 变化. 当恶意节点数量较低时, EFT-OLSR 比 FT-OLSR 性能更好. 原因是, 网络拓扑中的正常节点数远远大于恶意节点数时, 源节点在路由路径中有更多的备选节点, 获得更高的阈值, 恶意节点将从路径中删除, 使得 PDR 更高. 然而, 随着恶意节点数量的增加, 该网络拓扑已经完全失去了原有的构造, 被恶意节点肆意破坏, 采用的阈值变低, 使得 FT-OLSR 和 EFT-OLSR 的 PDR 基本相同.

2) 平均端到端延迟

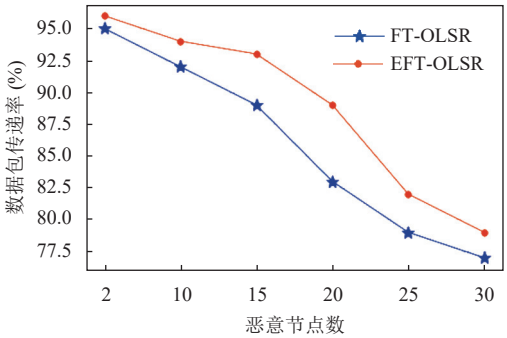
图 8(b) 显示了与 FT-OLSR 协议相比, 增加恶意节点数的 EFT-OLSR 协议平均端到端延迟. 结果表明, 在恶意节点数量较少的时候 EFT-OLSR 的端到端延迟略高, 因为为了保证较高的 PDR, 可能会让数据包沿着较长的路径避开恶意节点. 随着恶意节点的增加, FT-OLSR 开始高于 EFT-OLSR 的均端到端延迟, 因为 EFT-OLSR 虽花费更多时间寻找能够正确传递信息的路径, 但当恶意节点逐渐覆盖整个网络拓扑时, FT-OLSR 协议已经更加难以正确的传递数据包.

3) 丢包率

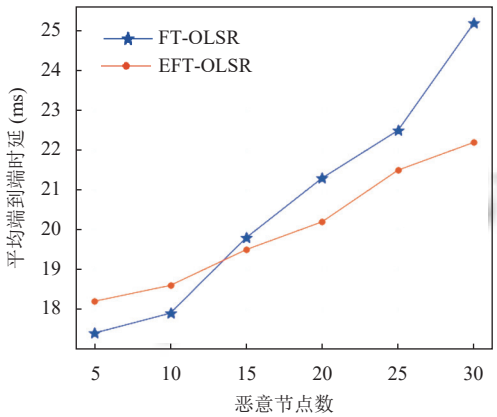
图 8(c) 显示了不同恶意节点下两种协议的丢包率. 从图中可以看出, 与 FT-OLSR 协议相比, 采用 EFT-OLSR 协议的丢包率更低. 原因是, 在 EFT-OLSR 协议下, 网络中的每个节点都在考虑其本地网络条件的情况下计算恶意节点隔离的阈值, 恶意节点被提前检测到. 然而 FT-OLSR 协议采用静态阈值, 容易误报恶意节点, 丢包率增加.



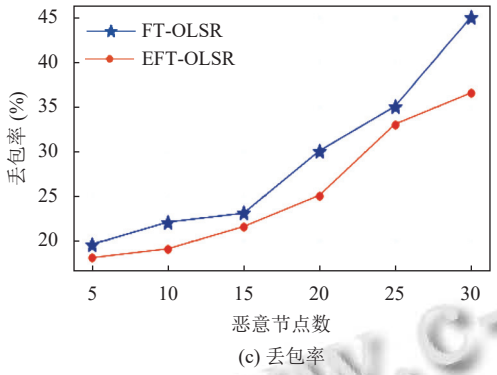
© 中国科学院软件研究所 http://www.c-s-a.org.cn




(a) 数据包传递率




(b) 平均端到端时延




(c) 丢包率

图 8 不同恶意节点数量的性能比较

## 4 结论

本文提出一种基于环境自适应决策的双层模糊逻辑信任 OLSR(EFT-OLSR) 作为原始 OLSR 的安全扩展协议.

(1) 通过模糊逻辑计算所属节点的可信度水平; 并根据网络环境中链路变化率、节点度、2 跳连通性, 构建出动态的信任阈值. 当一个节点的可信值小于阈值时, 该节点就被标记为恶意节点, 避免了恶意节点作为 MPR 节点, 有效的解决了黑洞攻击和自私攻击, 提高网络性能.

(2) 仿真结果表明, 本文提出的 EFT-OLSR 协议在数据包传递率、平均端到端时延、丢包率方面与 FT-OLSR 协议相比性能更好, 且降低了恶意节点的误报率.

(3) 当然本文提出的协议也有需要改进的地方, 如提取更多的参数, 加快信任机制的建立过程. 需研究和开发一个尽可能通用的信任模型, 有效检测和防止恶意节点发起的常见攻击.

## 参考文献

1 Ramphull D, Mungur A, Armoogum S, *et al*. A review of mobile ad hoc network (MANET) protocols and their applications. Proceedings of the 5th International Conference on Intelligent Computing and Control Systems (ICICCS). Madurai: IEEE, 2021. 204–211.

2 Al-Shakarchi SJH, Alubady R. A survey of selfish nodes detection in MANET: Solutions and opportunities of research. Proceedings of the 1st Babylon International Conference on Information Technology and Science (BICITS). Babil: IEEE, 2021. 178–184.

3 Lakrami F, Kamoun NEL, Labouidya O, *et al*. Analysis and evaluation of cooperative trust models in ad hoc networks: Application to OLSR routing protocol. Proceedings of the Advanced Intelligent Systems for Sustainable Development. Marrakech: Springer, 2019. 38–48.

4 Dehkordi AN, Adibnia F. Securing the OLSR routing protocol. OIC-CERT Journal of Cyber Security, 2020, 2(1): 77–86.

5 Sundaram BB, Elemo MTK. Node isolation attack on OLSR, reputation relied Mitigation. PalArch's Journal of Archaeology of Egypt/Egyptology, 2020, 17(9): 4549–4564.

6 Oyakhire O, Gyoda K. Improved OLSR considering node density and residual energy of nodes in dense networks. Proceedings of the 35th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC). Nagoya: IEEE, 2020. 161–165.

7 Semchedine F, Moussaoui A, Zouaoui K, *et al*. CRY OLSR: Crypto optimized link state routing for MANET. Proceedings of the 5th International Conference on Multimedia Computing and Systems. Marrakech: IEEE, 2016. 290–293.

8 Baadache A, Belmehdi A. Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. Computer Networks, 2014, 73: 173–184. [doi: 10.1016/j.comnet.2014.07.016]

9 Shcherba EV, Litvinov GA, Shcherba MV. A novel



© 中国科学院软件研究所 http://www.c-s-a.org.cn

reputation model for trusted path selection in the OLSR routing protocol. Proceedings of 2019 International Conference on Information Science and Communications Technologies (ICISCT). Tashkent: IEEE, 2019. 1–5.

10 Bhuvaneswari R, Ramachandran R. Denial of service attack solution in OLSR based manet by varying number of fictitious nodes. Cluster Computing, 2019, 22(S5): 12689–12699. [doi: 10.1007/s10586-018-1723-0]

11 Tu JB, Tian DH, Wang Y. An active-routing authentication scheme in MANET. IEEE Access, 2021, 9: 34276–34286. [doi: 10.1109/ACCESS.2021.3054891]

12 Khan MS, Midi D, Khan MI, *et al*. Adaptive trust threshold strategy for misbehaving node detection and isolation. Proceedings of 2015 IEEE Trustcom/BigDataSE/ISPA. Helsinki: IEEE, 2015. 718–725.

13 Paillassa B, Yawut C, Dhaou R. Network awareness and dynamic routing: The ad hoc network case. Computer Networks, 2011, 55(9): 2315–2328. [doi: 10.1016/j.comnet.2011.03.010]

14 Inedjaren Y, Zeddini B, Maachaoui M, *et al*. Securing intelligent communications on the vehicular ad hoc networks using fuzzy logic based trust OLSR. Proceedings of the IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). Abu Dhabi: IEEE, 2019. 1–6.

15 Ahmed A, Abu Bakar K, Channa MI, *et al*. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. Frontiers of Computer Science, 2015, 9(2): 280–296. [doi: 10.1007/s11704-014-4212-5]

16 Khan MS, Khan MI, Malik SUR, *et al*. MATF: A multi-attribute trust framework for MANETs. EURASIP Journal on Wireless Communications and Networking, 2016, 2016(1): 197. [doi: 10.1186/s13638-016-0691-4]

17 Wang CH. A study of membership functions on mamdani-type fuzzy inference system for industrial decision-making [Master's thesis]. Bethlehem: Lehigh University, 2015.

18 Wahengbam M, Marchang N. Intrusion Detection in MANET using fuzzy logic. Proceedings of the 3rd National Conference on Emerging Trends and Applications in Computer Science. Shillong: IEEE, 2012. 189–192.

19 Fathy C, El-Hadidi MT, El-Nasr MA. Fuzzy-based adaptive cross layer routing protocol for mobile ad hoc networks. Proceedings of the 30th IEEE International Performance Computing and Communications Conference. Orlando: IEEE, 2011. 1–10.

20 Sultana S, Ghinita G, Bertino E, *et al*. A lightweight secure provenance scheme for wireless sensor networks. Proceedings of the IEEE 18th International Conference on Parallel and Distributed Systems. Singapore: IEEE, 2012. 101–108.

21 Qin L, Kunz T. Mobility metrics to enable adaptive routing in MANET. Proceedings of 2006 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. Montreal: IEEE, 2006. 1–8.

22 Samar P, Wicker SB. On the behavior of communication links of a node in a multi-hop mobile environment. Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Roppongi Hills: ACM, 2004. 145–156.

(校对责编: 孙君艳)



© 中国科学院软件研究所 http://www.c-s-a.org.cn