基于动态信誉的无线 Mesh 网络安全路由机制

杨宏宇，韩越
（中国民航大学计算机科学与技术学院，天津 300300）

摘 要：针对无线 Mesh 网络安全路由机制匮乏、内部恶意节点在数据传输过程中容易产生分组丢失的问题，提出了一种基于动态信誉的无线 Mesh 网络安全路由机制（SRMDR）。首先，采用动态信誉机制评价节点行为，根据节点直接信誉值和推荐信誉值计算节点综合信誉值，整合节点历史综合信誉值与当前综合信誉值计算节点动态信誉值。然后，结合动态信誉机制和路由机制建立安全路由路径，将动态信誉值小于阈值的节点判定为恶意节点，并在路由过程中将其隔离。实验结果表明，与 HWMP、SHaRP 相比，SRMDR 具有较高的恶意节点识别率，并能有效减小分组丢失率，提高网络吞吐量。

关键词：无线 Mesh 网络；路由机制；恶意节点；主观逻辑；动态信誉
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019083

Wireless Mesh network secure routing mechanism based on dynamic reputation

YANG Hongyu, HAN Yue
College of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China

Abstract: Aiming at the problem that the wireless Mesh network (WMN) security routing mechanism was scarce and internal malicious nodes drop data packets during data transmission, a secure routing mechanism based on dynamic reputation (SRMDR) for wireless Mesh network was proposed. Firstly, the dynamic reputation mechanism was used to evaluate the node's behavior, the node's comprehensive reputation value was calculated according to the node's direct reputation value and the recommended reputation value, and the node's dynamic reputation value was calculated according to the node's historical comprehensive reputation value and the current comprehensive reputation value. Then, the dynamic reputation was combined with the routing mechanism to establish secure routing paths, the nodes with a dynamic reputation value less than the threshold were determined to be malicious nodes, which were isolated during the routing process. Experimental results show that compared with HWMP and SHaRP, SRMDR has higher malicious node recognition rates, and SRMDR can effectively reduce packet loss rate and improve network throughput.

Key words: wireless Mesh network, routing mechanism, malicious node, subjective logic, dynamic reputation

1 引言

随着网络技术的发展，无线 Mesh 网络（WMN, wirelss Mesh network）[1-2]被广泛应用于多个领域。WMN 传输介质的开放性和网络拓扑结构的动态性，使该网络极易遭受内部恶意节点的攻击。同时，由于内部恶意节点可以利用合法授权进行伪装，传统的路由机制无法在路由过程中将其准确识别，导

收稿日期：2018–11–12；**修回日期**：2019–01–31
基金项目：国家自然科学基金民航联合研究基金资助项目（No.U1833107）；国家科技重大专项基金资助项目（No.2012ZX03002002）
Foundation Items: The Civil Aviation Joint Research Fund Project of National Natural Science Foundation of China (No.U1833107), The National Science and Technology Major Project of China (No.2012ZX03002002)

致大量信息在路由传输过程中遭到破坏[3]，因此，如何在路由过程中有效识别恶意节点，构造安全的路由路径，成为目前 WMN 安全路由机制研究的热点。

Sarma 等[4]提出了一种基于安全分层和角色的安全路由协议（SHaRP, secure hierarchical and role based routing protocol），该协议在对路由控制信息进行加密的同时计算节点信誉值和链路的质量安全值，根据计算结果选出安全的路由路径。Bounouni 等[5]提出了一种节点信誉值与贡献值混合的确认方法（NHACK, new hybrid acknowledgment approach），采用基于监控确认技术的信誉值计算方法，并结合贡献系统计算节点在路由建立过程中的贡献值，依据节点信誉值与贡献值选出安全高效的路由路径。吴军等[6]提出了一种基于反馈可信度的可信机会路由转发模型，通过反馈可信度模型评价节点行为，进而识别出无线 Mesh 网络中的恶意节点，实现了路由过程中共谋攻击的防御。Guo 等[7]提出了一种基于信任机制的安全访问控制方案，采用基于贝叶斯理论的信任机制进行恶意节点识别，并采用改进 Diffie-Hellman 密钥协商协议实现路由过程中的密钥交换，保障路由信息的安全性。Sookhak 等[8]提出了一种无线网络恶意节点检测新方法，对数据分组标记的同时采用密钥预分配技术来进行恶意节点的识别，在不需要使用同步时钟等额外硬件的情况下实现对恶意节点的检测。上述研究成果虽然能够为无线 Mesh 网络的路由安全提供一定的保障，但仍存在以下不足：在路由过程中对节点的评价不够全面，缺乏时效性和动态性，没有结合节点历史行为与当前行为对节点做出综合评价，导致内部恶意节点的识别不够准确。

针对上述不足，本文将节点动态信誉值评价引入路由机制的设计中，提出了一种基于动态信誉的无线 Mesh 网络安全路由机制（SRMDR, secure routing mechanism based on dynamic reputation），通过动态信誉机制对节点做出综合评价，然后根据评价结果在路由过程中准确识别并隔离内部恶意节点，保障路由安全。

2 动态信誉机制

本文将主观逻辑理论[9]与信誉评价机制相结合，提出了一种新的动态信誉机制。依据路由过程中节点对数据分组的转发情况和链路质量进行信誉值评估，同时考虑节点信誉值随时间的变化，实时更新节点信誉值，最终准确识别出恶意节点，为路由选择提供依据。

节点 i 对节点 j 的信誉值评价可用四元组（$b_{i:j},d_{i:j},u_{i:j},a_{i:j}$）表示，四元组中的元素为 2 个节点间的信任度 $b_{i:j}$、不信任度 $d_{i:j}$、不确定度 $u_{i:j}$ 和信赖度 $a_{i:j}$。其中，$b_{i:j}$ 表示节点 i 对节点 j 的信任程度，$d_{i:j}$ 表示节点 i 对节点 j 的不信任程度，$u_{i:j}$ 表示节点 i 对节点 j 信任中的不确定程度，$a_{i:j}$ 表示节点 i 愿意相信节点 j 是可信节点的程度。为避免其他因素干扰，保证节点评价的客观性，本文默认 $a_{i:j}$=0.5 并统一用 a 表示，其他各元素满足式(1)所示的条件[10]。

$$\begin{cases} b_{i:j}+d_{i:j}+u_{i:j}=1.0 \\ b_{i:j},d_{i:j},u_{i:j}\in[0.0,1.0] \end{cases} \tag{1}$$

本文提出的动态信誉机制中需要计算的节点信誉值包括直接信誉值、推荐信誉值、综合信誉值和动态信誉值。具体计算过程如下。

1) 根据节点对数据分组的转发情况和链路质量，计算节点的直接信誉值。

2) 结合邻居节点的推荐信息，计算节点的推荐信誉值。

3) 根据节点的直接信誉值和推荐信誉值，计算节点的综合信誉值。

4) 整合节点的历史综合信誉值和当前综合信誉值，计算节点的动态信誉值。

2.1 直接信誉值计算

直接信誉值 $T_{i:j}^{\mathrm{dir}}$ 表示当前时刻节点 i 对节点 j 信誉值的直接评价，评价结果存储在节点本地数据库中。在路由过程中，源节点发出的数据分组经节点 i 传递给邻居节点 j。节点 i 在传递数据分组的同时对节点 j 的转发情况进行监视，根据监视结果计算出节点 j 的直接信誉值 $T_{i,j}{}^{\mathrm{dir}}$ 为

$$T_{i:j}^{\mathrm{dir}}=b_{i:j}^{\mathrm{dir}}+au_{i:j}^{\mathrm{dir}} \tag{2}$$

其中，$b_{i:j}^{\mathrm{dir}}$、$d_{i:j}^{\mathrm{dir}}$ 和 $u_{i:j}^{\mathrm{dir}}$ 分别为

$$\begin{cases} b_{i:j}^{\mathrm{dir}}=\dfrac{s_{i:j}}{(s_{i:j}+f_{i:j})L_{i:j}} \\ d_{i:j}^{\mathrm{dir}}=\dfrac{f_{i:j}}{(s_{i:j}+f_{i:j})L_{i:j}} \\ u_{i:j}^{\mathrm{dir}}=1.0-b_{i:j}^{\mathrm{dir}}-d_{i:j}^{\mathrm{dir}} \end{cases} \tag{3}$$

其中，$s_{i:j}$ 表示节点 j 从节点 i 接收到的数据分组中成功转发的数量，$f_{i:j}$ 表示节点 j 从节点 i 接收到的数据分组中丢弃的数量，$L_{i:j}$ 表示节点 i 与节点 j 之间无线链路的链路质量，计算式为

$$\begin{cases} L_{i:j} = p_{i:j} p_{j:i} \\ p = \dfrac{k_{\mathrm{s}}}{k_{\mathrm{t}}} \end{cases} \tag{4}$$

其中，$P_{i:j}$ 表示节点 i 与节点 j 之间无线链路的正向传输率，$P_{j:i}$ 表示节点 i 与节点 j 之间无线链路的反向传输率，k_{t} 表示无线链路两端的发送节点在一次传输过程中共发送的数据分组数量，k_{s} 表示无线链路两端的接收节点在一次传输过程中共接收到的数据分组数量。

2.2　推荐信誉值计算

由于节点 i 可能没有足够的历史交互数据来评价节点 j，且计算出的直接信誉值无法对节点 j 做出全面的判断，因此节点 i 会向邻居节点发起推荐信誉值计算过程，进一步对节点 j 进行评价。推荐信誉值的具体计算过程为：节点 i 向邻居节点广播发送信誉值查询信息，发起推荐信誉值计算过程；节点 i 的邻居节点收到查询信息后，查询本地记录，如果存在关于节点 j 的信誉值，则发送响应消息，将节点 j 的直接信誉值计算结果发送给节点 i；若节点 i 的邻居节点中有 n（n>2）个节点的信誉值数据库中存在对节点 j 的直接信誉值计算结果，则对于每个推荐者 m，首先由式(5)计算相应的权重因子 h_m 为

$$h_m = \frac{T_{i:m}^{\mathrm{dir}}}{\sum_{m=1}^{n} T_{i:m}^{\mathrm{dir}}} \tag{5}$$

其中，$T_{i:m}^{\mathrm{dir}}$ 表示节点 i 对节点 m 的直接信誉值计算结果，值越大，表示节点 m 的可信程度越高，相应的加权因子 h_m 越大，节点 m 的推荐意见在最终的推荐信誉值中所占的比重也越大。

由于恶意节点在转发过程中会丢弃部分数据分组，因此它们的直接信誉值 T^{dir} 会很小。在推荐信誉值计算过程中，这些恶意节点的推荐信息对信誉值计算的影响就会很小，从而保证最终的综合推荐信誉值更加准确。

得到加权因子后，由式(6)对接收到的所有推荐信息进行整合。

$$\begin{cases} b_{i:j}^{\mathrm{ind}} = \dfrac{\sum_{m=1}^{n} h_m b_{m:j}^{\mathrm{dir}}}{n} \\ d_{i:j}^{\mathrm{ind}} = \dfrac{\sum_{m=1}^{n} h_m d_{m:j}^{\mathrm{dir}}}{n} \\ u_{i:j}^{\mathrm{ind}} = \dfrac{\sum_{m=1}^{n} h_m u_{m:j}^{\mathrm{dir}}}{n} \end{cases} \tag{6}$$

整合完成后，计算出节点的最终推荐信誉值 $T_{i:j}^{\mathrm{ind}}$ 为

$$T_{i:j}^{\mathrm{ind}} = b_{i:j}^{\mathrm{ind}} + a u_{i:j}^{\mathrm{ind}} \tag{7}$$

2.3　综合信誉值计算

得到节点的直接信誉值和推荐信誉值后，计算节点的综合信誉值 $T_{i:j}^{\mathrm{syn}}$ 为

$$T_{i:j}^{\mathrm{syn}} = b_{i:j}^{\mathrm{syn}} + a u_{i:j}^{\mathrm{syn}} \tag{8}$$

其中，$b_{i:j}^{\mathrm{syn}}$、$d_{i:j}^{\mathrm{syn}}$ 和 $u_{i:j}^{\mathrm{syn}}$ 分别为[11]

$$\begin{cases} b_{i:j}^{\mathrm{syn}} = \dfrac{b_{i:j}^{\mathrm{dir}} u_{i:j}^{\mathrm{ind}} + b_{i:j}^{\mathrm{ind}} u_{i:j}^{\mathrm{dir}}}{u_{i:j}^{\mathrm{dir}} + u_{i:j}^{\mathrm{ind}} - u_{i:j}^{\mathrm{dir}} u_{i:j}^{\mathrm{ind}}} \\ d_{i:j}^{\mathrm{syn}} = \dfrac{d_{i:j}^{\mathrm{dir}} u_{i:j}^{\mathrm{ind}} + d_{i:j}^{\mathrm{ind}} u_{i:j}^{\mathrm{dir}}}{u_{i:j}^{\mathrm{dir}} + u_{i:j}^{\mathrm{ind}} - u_{i:j}^{\mathrm{dir}} u_{i:j}^{\mathrm{ind}}} \\ u_{i:j}^{\mathrm{syn}} = \dfrac{u_{i:j}^{\mathrm{dir}} u_{i:j}^{\mathrm{ind}}}{u_{i:j}^{\mathrm{dir}} + u_{i:j}^{\mathrm{ind}} - u_{i:j}^{\mathrm{dir}} u_{i:j}^{\mathrm{ind}}} \end{cases} \tag{9}$$

当 $u_{i:j}^{\mathrm{dir}} + u_{i:j}^{\mathrm{ind}} - u_{i:j}^{\mathrm{dir}} u_{i:j}^{\mathrm{ind}} = 0$ 时，$b_{i:j}^{\mathrm{syn}}$、$d_{i:j}^{\mathrm{syn}}$ 和 $u_{i:j}^{\mathrm{syn}}$ 分别为

$$\begin{cases} b_{i:j}^{\mathrm{syn}} = \dfrac{\gamma b_{i:j}^{\mathrm{dir}} + b_{i:j}^{\mathrm{ind}}}{\gamma + 1} \\ d_{i:j}^{\mathrm{syn}} = \dfrac{\gamma d_{i:j}^{\mathrm{dir}} + d_{i:j}^{\mathrm{ind}}}{\gamma + 1} \\ u_{i:j}^{\mathrm{syn}} = u_{i:j}^{\mathrm{dir}} = u_{i:j}^{\mathrm{ind}} = 0 \end{cases} \tag{10}$$

其中，γ 代表权重因子，表示直接信任度对综合信任度的影响程度。

2.4　动态信誉值计算

无线 Mesh 网络中节点的行为会随时间的推移发生变化，之前计算的节点信誉值对节点的评价作用会随时间发生衰减，不能真实地体现节点当前的

状态。当前计算的节点信誉值没有考虑节点的历史表现，对节点的评价不够全面，因此，为了保障节点评价的动态性和全面性，需要计算节点的动态信誉值 $\mathrm{Dyn}T_{i:j}^{\mathrm{syn}}$。$\mathrm{Dyn}T_{i:j}^{\mathrm{syn}}$ 综合考虑节点的历史综合信誉值 $\mathrm{Old}T_{i:j}^{\mathrm{syn}}$ 和当前综合信誉值 $\mathrm{New}T_{i:j}^{\mathrm{syn}}$，使节点的评价更加全面准确。假设节点的信誉值计算间隔为 10 s，则 $\mathrm{Old}T_{i:j}^{\mathrm{syn}}$ 为节点 10 s 前的综合信誉值，$\mathrm{New}T_{i:j}^{\mathrm{syn}}$ 为节点当前的综合信誉值。$\mathrm{Dyn}T_{i:j}^{\mathrm{syn}}$ 的计算式为

$$\mathrm{Dyn}T_{i:j}^{\mathrm{syn}}=\tau\omega_1\mathrm{Old}T_{i:j}^{\mathrm{syn}}+\omega_2\mathrm{New}T_{i:j}^{\mathrm{syn}} \tag{11}$$

其中，ω_1 和 ω_2 为权重因子，由于当前综合信誉值比历史综合信誉值具有更高的参考价值，因此 ω_1 和 ω_2 需满足 $0<\omega_1<\omega_2<1$，$\omega_1+\omega_2=1$；τ 为衰减因子，表示历史信誉值随时间的衰减程度，且 $0<\tau<1$。

3 安全路由机制

本文将动态信誉机制应用于无线 Mesh 网络路由过程，提出了一种基于动态信誉的安全路由机制（SRMDR）。该机制由路由建立和路由维护这 2 个阶段组成。

3.1 路由建立

SRMDR 通过源节点广播路由请求（RREQ, route request）信息发起路由建立，源节点构建 RREQ 信息，并向邻居节点广播发送。邻居节点收到源节点发来的 RREQ 信息，通过动态信誉机制判断源节点是否可信，随后向源节点发送路由响应（RREP, route respond）信息进行响应。假设节点信誉值的阈值为 β（$\beta\in[0.0, 1.0]$），SRMDR 路由建立的具体过程设计如下。

步骤 1 源节点 j 生成 RREQ 信息，并广播发送给邻居节点。

步骤 2 节点 j 的任意邻居节点 i 收到 RREQ 信息后，采用动态信誉机制对节点 j 进行评价，鉴别其是否为可信节点。具体过程如下。

1) 节点 i 查询本地信誉值数据库，搜寻有关节点 j 的数据分组转发信息。根据查询结果计算节点 j 的直接信誉值 $T_{i:j}^{\mathrm{dir}}$，并将其保存在本地信誉值数据库中。

2) 若 $T_{i:j}^{\mathrm{dir}}<\beta$，则判定节点 j 为恶意节点并将其隔离；若 $T_{i:j}^{\mathrm{dir}}>\beta$ 或者没有足够的数据进行 $T_{i:j}^{\mathrm{dir}}$ 的计算，则执行步骤 3)进行判断。

3) 节点 i 向邻居节点广播信誉值查询信息，要求提供关于节点 j 的推荐信息，发起推荐信誉值计算过程。

4) 节点 i 和节点 j 的任意共同邻居节点 m 收到信誉值查询信息后，查询本地信誉值数据库并将查询结果反馈给节点 i。

5）节点 i 将收到的所有邻居节点反馈的推荐信息进行整理，计算出节点 j 的推荐信誉值 $T_{i:j}^{\mathrm{ind}}$。

6) 节点 i 根据计算得出的直接信誉值和推荐信誉值，计算节点 j 的综合信誉值 $T_{i:j}^{\mathrm{syn}}$，即为节点 j 的当前综合信誉值 $\mathrm{New}T_{i:j}^{\mathrm{syn}}$。再结合信誉值数据库中节点 j 的历史综合信誉值 $\mathrm{Old}T_{i:j}^{\mathrm{syn}}$，计算节点的动态信誉值 $\mathrm{Dyn}T_{i:j}^{\mathrm{syn}}$。

7) 若 $\mathrm{Dyn}T_{i:j}^{\mathrm{syn}}<\beta$，则节点 i 判定节点 j 为恶意节点并将其隔离；若 $\mathrm{Dyn}T_{i:j}^{\mathrm{syn}}>\beta$，则判定节点 j 为可信节点并向其发送 RREP 消息。

步骤 3 节点 j 收到 RREP 消息后，执行步骤 2 来判断节点 i 是否为可信节点。若节点 j 将节点 i 判定为可信节点，则将其作为路由中的下一跳节点进行数据传递，否则将其隔离。

步骤 4 循环执行步骤 2 和步骤 3，直到找出源节点到目的节点之间符合要求的路由路径。

步骤 5 如果存在多条符合要求的路径，则选择节点平均动态信誉值最高的路径作为最终的安全路径。节点的平均动态信誉值通过路径中所有节点的动态信誉值之和除以节点数量来计算。

3.2 路由维护

由于无线 Mesh 网络存在动态性，节点的行为会随时间发生变化，已建立的安全路由路径会遭到破坏，因此路由的维护过程也变得同等重要。假设 l、m、n 为已建立的路由路径上的任意相邻节点，SRMDR 路由维护的具体过程设计如下。

步骤 1 节点 m 定期计算上一跳节点 l 的动态信誉值 $\mathrm{Dyn}T_{m:l}^{\mathrm{syn}}$ 并与阈值 β 比较。若 $\mathrm{Dyn}T_{m:l}^{\mathrm{syn}}>\beta$，则接收来自节点 l 的数据分组，并执行步骤 2 判断下一跳节点 n 是否为可信节点；若 $\mathrm{Dyn}T_{m:l}^{\mathrm{syn}}<\beta$，则停止接收来自节点 l 的数据分组，并向源节点发送路由维护消息。

步骤 2 节点 m 计算下一跳节点 n 的动态信誉值 $\mathrm{Dyn}T_{m:n}^{\mathrm{syn}}$ 并与阈值 β 比较。若 $\mathrm{Dyn}T_{m:n}^{\mathrm{syn}}>\beta$，则继续将节点 n 作为下一跳节点，并将数据分组发送给节点 n；若 $\mathrm{Dyn}T_{m:n}^{\mathrm{syn}}<\beta$，则停止向节点 n 发送数据分组，并向源节点发送路由维护消息。

步骤 3　源节点收到路由维护消息后，首先广播通知所有节点对新发现的恶意节点进行记录并予以隔离，然后重新发起路由建立的过程，建立新的安全路由路径。

4　实验与结果

在 NS2 仿真环境中获取 SRMDR、混合无线 Mesh 协议（HWMP, hybrid wireless Mesh protocol）、SHaRP[4]这 3 种路由机制的恶意节点识别率、网络吞吐量和端到端平均时延的指标数据，并对仿真实验结果进行对比和分析。

采用网络仿真工具 NS2（NS-2.35）[12]进行仿真实验，通过 Matlab（Matlab R2016a）对实验结果进行处理和展示。

NS2 环境设置与实验过程如下。

1) 编写 OTcl 脚本，生成一个 900 m×900 m 的模拟区域，设置追踪文件监测数据分组传递情况。

2) 生成 60 个网络节点，随机分布在模拟区域中，节点的网络布局如图 1 所示。由于本文提出的 SRMDR 不受节点分布影响，因此随机分布节点的网络布局对实验结果不会产生影响。

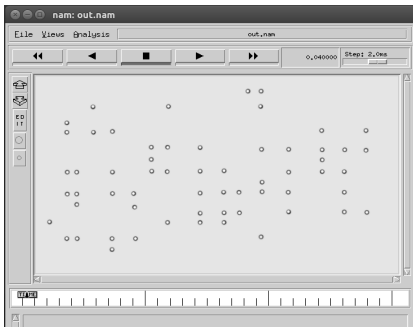

图 1　NS2 中节点的网络布局

3) 设置节点的通信半径为 200 m。

4) 设置 MAC 层采用 IEEE 802.11 的无线网络通用标准。

5) 设定流量传输模型为恒定比特率模型。

6) 将编写的 SRMDR 源码文件夹添加到 NS2 的 ns-allinone-2.35/ns-2.35 目录中，在 PT_NTYPE 之前加入 PT_SRMDR，将 PT_SRMDR 添加到 commom/packet.h 文件列表中，并在 p_info 类中定义新的分组类 name_[PT_SRMDR]="srmdr"。

7) 在 trace/cmu-trace.cc 的 format（）函数中添加 case PT_SRMDR，记录分组信息，编译 priqueue.cc 文件中的 recv（）函数声明队列优先级。

8) 修改 OTcL 库文件，在 tcl/lib/ns-packet.tcl 中添加 SRMDR，设定属性默认值，修改 Makefile 中的 OBJ_CC 变量，编译新添加的文件，得到 trace 跟踪文件。

9)利用 gawk 分析 trace 跟踪文件，提取实验结果数据，然后采用 Matlab 对数据进行图形化展示。

实验参数设置如表 1 所示。

表 1　　**实验参数**

参数	取值
仿真区域大小	900 m×900 m
实验时间/s	100
MAC 层	IEEE 802.11
权重 γ	0.5
权重 ω_1 和 ω_2	0.6 和 0.4
节点数/个	60
流量类型	固定码率流
信誉值阈值 β	0.6
信赖度 a	0.5
衰减因子 τ	0.98

4.1　恶意节点识别率

恶意节点识别率是指被识别出的恶意节点数占恶意节点总数的比率。本文实验通过比较 3 种路由机制的恶意节点识别率随时间的变化情况，分析 SRMDR 准确识别恶意节点的能力。实验过程设计如下。

步骤 1　设置节点信誉值阈值为 0.6，并作为恶意节点判定依据。

步骤 2　在生成的 60 个节点中，随机选取 20 个节点设置为具有分组丢失行为的恶意节点。

步骤 3　当实验时间 t=0~10 s 时，节点开始传输数据，传输节点计算相邻节点综合信誉值并与阈值比较，开启恶意节点识别过程。

步骤 4　设置动态信誉值计算周期为 10 s，当 t=20 s 时，传输节点结合相邻节点历史综合信誉值与当前综合信誉值，计算相邻节点动态信誉值并与阈值比较，进一步识别恶意节点。

步骤 5　统计网络识别出的恶意节点数，由恶意节点识别率=$\frac{\text{识别出的恶意节点数}}{\text{恶意节点总数}}$，依次计算 t=20 s、40 s、…、100 s 时, SRMDR 的恶意节点识别率。

步骤 6　在相同环境下分别加载 HWMP 和 SHaRP，计算这 2 种路由机制相应时刻的恶意节点识别率并与 SRMDR 比较。

随着时间的变化，3 种路由机制的恶意节点识

别率变化情况如图 2 所示。

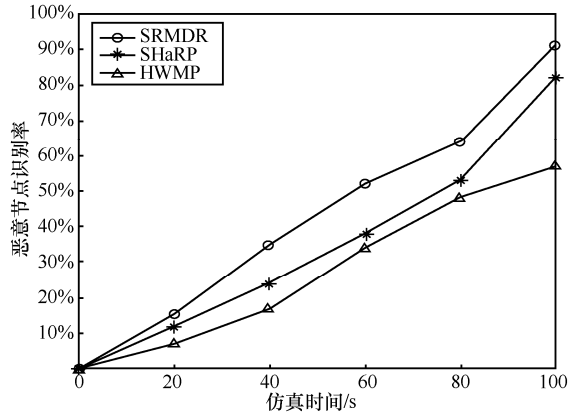

图 2 3 种路由机制的恶意节点识别率变化情况

由图 2 可知，在实验的初始阶段，3 种路由机制的恶意节点识别率都不高且比较接近。随着时间的增加，3 种路由机制的恶意节点识别率都逐渐增加且 SRMDR 的恶意节点识别率高于其他 2 种路由机制。这是因为初始阶段节点间交互行为较少，可用于计算节点信誉值的依据不足。随着时间的增加，节点信誉值计算过程不断完善，同时由于 SRMDR 采用动态信誉机制，综合考虑节点的历史信誉值和当前信誉值，使节点评价具有实时性且更加全面。因此，随着时间的增加，相对于其他 2 种路由机制，SRMDR 可以更加及时准确地识别出恶意节点。

4.2 网络吞吐量

网络吞吐量是指网络节点单位时间内成功传输的数据量。本文实验通过比较 3 种路由机制的网络吞吐量随恶意节点数的变化情况，分析 SRMDR 在恶意节点影响下保证网络吞吐量的能力。实验过程设计如下。

步骤 1 分别在实验环境中设置 2、4、…、20 个恶意节点。

步骤 2 恶意节点在数据传输过程中随机产生分组丢失行为，设置恶意节点的分组丢失率为 20%~60%。

步骤 3 经过 100 s 后，统计网络中传输的数据量。

步骤 4 由网络吞吐量=$\frac{\text{网络传输的数据量}}{\text{传输时间}}$，分别计算当网络中的恶意节点数量为 2、4、…、20 个时，3 种路由机制各自的网络吞吐量。

随着恶意节点数量的变化，3 种路由机制的网络吞吐量变化情况如图 3 所示。

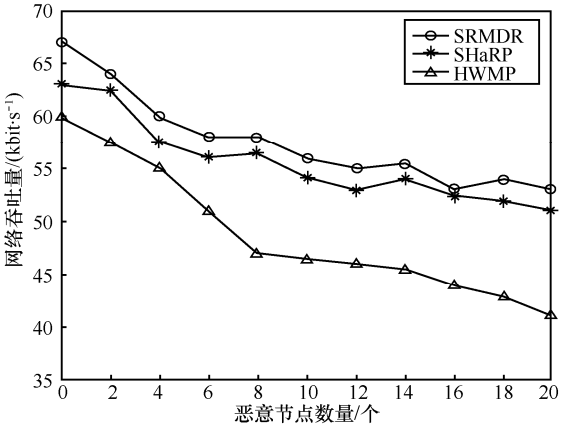

图 3 3 种路由机制的网络吞吐量变化情况

由图 3 可知，随着恶意节点数量的增加，3 种路由机制下的网络吞吐量都有所下降，但在具有相同数量恶意节点的网络环境中，SRMDR 的网络吞吐量相对较高。这是因为恶意节点数量越多，网络重新建立路由的概率越大，网络的传输效率越低。但在恶意节点数量相同的情况下，SRMDR 根据节点对数据的转发行为和链路质量对节点的信誉做出全面评价，从而更加有效、灵活地识别出网络中的恶意节点，减小数据分组在转发过程中被丢弃的概率，有效改善网络的传输效率，提高网络的吞吐量。

4.3 端到端平均时延

端到端平均时延是指数据分组从源节点传输到目的节点所需要的平均时间。本文实验通过比较 3 种路由机制的端到端平均时延随恶意节点数的变化情况，分析 SRMDR 传送数据所需的时间开销。实验过程设计如下。

步骤 1 设置实验环境中数据的传输速率为 11 Mbit/s。

步骤 2 统计每个数据分组从源节点开始发送的时间。

步骤 3 统计每个数据分组经过网络传输后，到达目的节点的时间。

步骤 4 待数据传输完成，由数据分组传输时间=数据分组到达时间−数据分组发送时间，分别计算每个数据分组的传输时间并求和。

步骤 5 统计整个传输过程中网络传输数据分组的总数。

步骤 6 根据端到端的平均时延=$\frac{\text{数据分组传输时间之和}}{\text{数据分组总数}}$，分别计算当恶意节点数量为 0、5、…、30 个时，3 种路由机制网络传输的端

到端平均时延。

随着恶意节点数量的变化，3 种路由机制的端到端平均时延变化情况如图 4 所示。

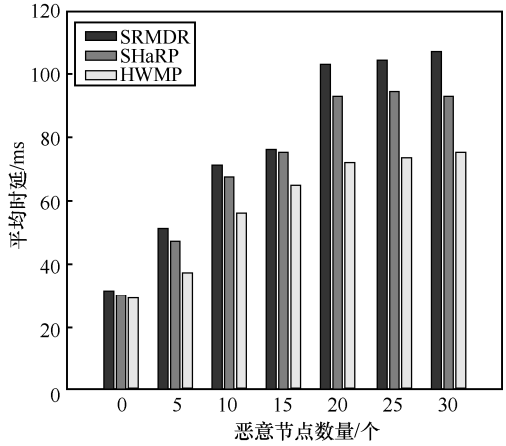

图 4　3 种路由机制的端到端平均时延变化情况

由图 4 可知，随着网络中恶意节点数量的增加，3 种路由机制的平均时延都出现增长，原因是恶意节点增多导致路由建立过程所需的时间增长，平均时延随之增加。在恶意节点数量相同的情况下，SRMDR 的平均时延高于其他 2 种路由机制，原因是 SRMDR 在路由建立过程中综合评估节点的当前信誉值和历史信誉值，增加了一定时间开销。但这种额外开销仍处于一般网络服务许可范围内，且不会显著影响网络传输效率。此外，正是由于 SRMDR 采用动态信誉机制对节点行为和链路质量进行全面的评价，使路由过程中节点的质量和数据的安全性得到保障。

5　结束语

本文针对无线 Mesh 网络安全路由机制匮乏、内部恶意节点在数据传输过程中容易产生分组丢失的问题，提出了一种基于动态信誉的无线 Mesh 网络安全路由机制——SRMDR。SRMDR 采用动态信誉机制，根据节点对数据的转发行为和链路质量对节点的信誉进行全面评价，依据评价结果识别并隔离恶意节点，最终利用可信节点在路由的建立与维护过程中传递数据。与 HWMP、SHaRP 机制相比，SRMDR 具有较高的恶意节点识别率，并能有效降低数据分组在路由传输过程中的分组丢失率，提高网络吞吐量。

在未来工作中，将研究降低 SRMDR 时间开销的方法，进一步提高 SRMDR 的运行效率。

参考文献：

[1] 杨宏宇, 李航. 无线 Mesh 网络恶意节点检测模型[J]. 清华大学学报(自然科学版), 2017, 57(7): 687-694.
YANG H Y, LI H. Malicious node detection model for wireless Mesh networks[J]. Journal of Tsinghua University (Science and Technology), 2017, 57(7): 687-694.

[2] BARGHI H, AZHARI V. A practical sleep coordination and management scheme with duty cycle control for energy sustainable IEEE 802.11s wireless mesh networks[J]. Wireless Networks, 2018, 12(4): 1-26.

[3] MALARVIZHI L, GOPALAKRISHNAN V. Malicious node detection scheme for upgraded femtocell architecture in wireless mesh networks[J]. Journal of Computational & Theoretical Nanoscience, 2016, 13(7): 4573-4579.

[4] SARMA D, KAR A, MALL R. A hierarchical and role based secure routing protocol for mobile wireless sensor networks[J]. Wireless Personal Communications, 2016, 90(3): 1067-1103.

[5] BOUNOUNI M, BOUALLOUCHE-MEDJKOUNE L. A hybrid stimulation approach for coping against the malevolence and selfishness in mobile Ad Hoc network[J]. Wireless Personal Communications, 2016, 88(2): 255-281.

[6] 吴军, 莫伟伟, 印新棋, 等. 基于反馈可信度的可信机会路由转发模型[J]. 计算机工程与应用, 2017, 53(8): 23-28.
WU J, MO W W, YIN X Q, et al. Trusted opportunistic routing forwarding model based on feedback credibility[J]. Computer Engineering and Applications, 2017, 53(8): 23-28.

[7] GUO J, ZHOU X, YUAN J, et al. Secure access control guarding against internal attacks in distributed networks[J]. Wireless Personal Communications, 2013, 68(4): 1595-1609.

[8] SOOKHAK M, AKHUNDZADA A, SOOKHAK A, et al. Geographic wormhole detection in wireless sensor networks[J]. Plos One, 2015, 10(1): 77-98.

[9] HOOGH J, ZANNONE N. Flow-based reputation with uncertainty: evidence-based subjective logic[J]. International Journal of Information Security, 2016, 15(4): 381-402.

[10] CHO H. Dynamics of uncertain and conflicting opinions in social networks[J]. IEEE Transactions on Computational Social Systems, 2018, 5(2): 518-531.

[11] 林晖, 马建峰. 无线 Mesh 网络中基于跨层信誉机制的安全路由协议[J]. 西安电子科技大学学报, 2014, 41(1): 116-123.
LIN H, MA J F. Cross layer reputation mechanism based secure routing protocol for WMNs[J]. Journal of Xidian University, 2014, 41(1): 116-123.

[12] PLOUMIDIS M, PAPPAS N, TRAGANITIS A. Flow allocation for maximum throughput and bounded delay on multiple disjoint paths for random access wireless multihop networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(1): 720-733.

[作者简介]

杨宏宇（1969− ），男，吉林长春人，博士，中国民航大学教授，主要研究方向为网络信息安全、移动系统安全等。

韩越（1990− ），男，河北承德人，中国民航大学硕士生，主要研究方向为网络信息安全。