计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2015.20140606
52(8):1883-1892,2015

HWMN 中一种新的隐私感知安全路由协议

林 晖[1] 田有亮[2] 许 力[1] 胡 嘉[3]
[1](福建省网络安全与密码技术重点实验室(福建师范大学数学与计算机科学学院) 福州 350117)
[2](贵州大学理学院 贵阳 550025)
[3](利物浦霍普大学数学与计算机科学系 英国利物浦 L16 9JD)
(tianyouliang@iie.ac.cn)

A Novel Privacy Aware Secure Routing Protocol for HWMN

Lin Hui[1], Tian Youliang[2], Xu Li[1], and Hu Jia[3]
[1](*Fujian Provincial Key Laboratory of Network Security and Cryptology* (*School of Mathematics and Computer Science*, *Fujian Normal University*), *Fuzhou* 350117)
[2](*College of Science*, *Guizhou University*, *Guiyang* 550025)
[3](*Department of Mathematics and Computer Science*, *Liverpool Hope University*, *Liverpool*, *UK L16 9JD*)

Abstract Hybrid wireless mesh network (HWMN) is the most practical architecture in wireless mesh networks (WMNs), which provides a fusion of heterogeneous wireless networks, network connectivity and coverage to distributed users in a wide area to support applications in different domains, such as military, finance and healthcare. Due to the multi-hop and decentralized network architecture, HWMN is susceptible to various security threats, especially to the internal attacks aiming to the routing and privacy security. However, existing routing protocols for HWMN cannot ensure the security and protect the user privacy effectively as they are vulnerable to internal attacks. Moreover, few of them have taken the energy consumption into account at routing. To solve the above problem, combining with the characters of the HWMN, this paper proposes a dynamic reputation mechanism based privacy aware secure routing protocol (RPASRP), which combines a new dynamic reputation mechanism with the hierarchical key management protocol and hierarchical encryption scheme. Furthermore, the energy consumption is taken into account in the process of routing. Simulation results show that RPASRP can implement the security and privacy protection against the inside attacks more effectively and decrease the energy consumption in the process of routing.

Key words hybrid wireless mesh network (HWMN); secure routing protocol; privacy preserving; reputation mechanism; energy consumption

摘 要 混合无线 Mesh 网络(hybrid wireless mesh network, HWMN)是最具实际应用前景的无线 Mesh 网(wireless mesh networks, WMNs)结构.然而,HWMN 也面临着各种安全威胁,尤其是针对路由和隐私安全的内部攻击的威胁.针对这一问题,结合 HWMN 的特点,提出了基于动态信誉机制的隐私感知安全路由协议(dynamic reputation based privacy-aware secure routing protocol, RPASRP).RPASRP 实现了动态信誉机制、分级密钥管理协议与路由协议的有机结合,并充分考虑了路由过程中的能量损耗.仿真结果表明,RPASRP 能有效抵御内部攻击、实现隐私保护和减少路由能量损耗.

收稿日期:2014-07-07;**修回日期**:2014-11-20
基金项目:国家自然科学基金青年科学基金项目(61202450,61363068);国家自然科学基金面上基金项目(61472083);福建省自然科学基金项目(2014J01223)
通信作者:田有亮(tianyouliang@iie.ac.cn)

关键词 混合无线 Mesh 网络;安全路由协议;隐私保护;信誉机制;能量损耗

中图法分类号 TP309

混合无线 Mesh 网络(hybrid wireless mesh network, HWMN),如图 1 所示,是无线 Mesh 网络(wireless mesh networks, WMNs)中具有最佳与最广泛应用前景的网络结构[1]. 随着 HWMN 应用领域的扩大,其面临的安全威胁日益突出. 同时,大量的隐私信息将出现在网络中,这些隐私信息的泄露将给个人、社会和国家带来严重的后果. 因此,提供网络与隐私安全保障是 HWMN 能够进一步发展的前提和基础[2].

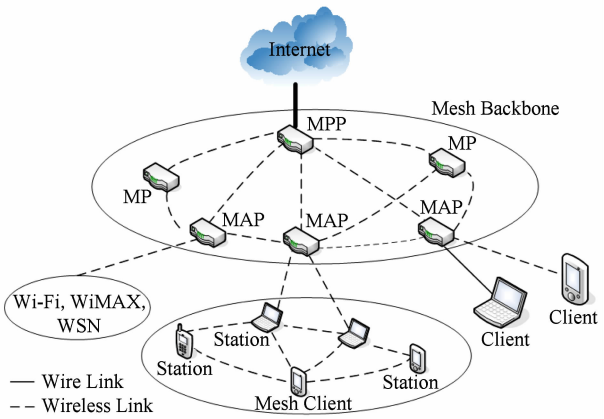


Fig. 1 HWMN structure.

图 1 混合无线 Mesh 网络结构

HWMN 中,路由协议作为重要的组成部分,一直是各种网络攻击,尤其是内部攻击的主要对象[3]. 由于 HWMN 中信息的完整性、机密性和隐私性贯穿数据流传输的全过程,内部发起的各种路由攻击,将破坏信息的完整性和机密性,泄漏隐私信息[2,4]. 因此,设计能够有效防御内部攻击和保护隐私的安全路由协议是 HWMN 必须重点关注和解决的问题[5-6].

本文在全面分析 HWMN 及存在的网络和隐私安全问题的基础上,提出了基于动态信誉机制的隐私感知安全路由协议(dynamic reputation mechanism based privacy aware secure routing protocol, RPASRP). 本文的贡献包括:1)考虑了时间对信誉度的影响,提出了基于主观逻辑的动态信誉机制,使得信誉度的评估结果能够动态地、更准确地反映节点的行为,从而提高对恶意节点识别的准确性;2)采用新的恶意节点分类和管理机制,对恶意节点实施灵活的管理,增强了 HWMN 的容错能力和生存能力;3)设计了新的分级密钥管理协议,对数据传输过程进行保护,从而实现隐私安全保护;4)将能量损耗问题引入路由,提出节点能耗评估模型和基于节点能耗的路径选择机制,使得 RPASRP 同时满足安全和节能的需求;5)采用优化网络工程仿真工具(optimized network engineering tool, OPNET)进行了详细的仿真验证和性能分析.

1 相关工作

近些年来,尽管出现了许多基于骨干和终端 WMNs 网络结构的安全路由协议,但是,HWMN 特殊的网络结构和通信方式,特别是终端网络的自组织特点,使得这些成果无法被直接地应用. 因此,人们开始研究 HWMN 中的安全路由协议.

文献[7]中,Islam 等人提出了一种安全的混合无线 Mesh 网络路由协议(secure hybrid wireless mesh protocol, SHWMP). SHWMP 通过使用加密扩展的方法来保证路由信息的可靠性和完整性,防止对路由信息中可修改字段的未授权操作. 文献[8]中,Ren 等人提出了一种应用于 HWMN 的隐私增强的安全架构(privacy-enhanced yet accountable security framework, PEACE),并将 PEACE 应用于安全路由协议的设计. PEACE 基于内部节点都是可信和协作的假设,设计了基于短群签名的认证和密钥协商协议,实现了对外部攻击的防御. Sen 在文献[9-10]中针对 HWMN 提出了一种有效的可靠的匿名路由协议. 该协议通过对路由路径上的无线链路质量和可用带宽的估计以及通过使用多点中继和循环路由技术,使得该路由协议能够花费较少的控制开销就维持 1 个较高水平的网络吞吐量. 用户的隐私则通过使用匿名认证协议来保护. 文献[3-4]中,Khan 等人针对 HWMN 分别提出了增强的无线网状网安全路由协议(enhanced secure routing protocol for wireless mesh network, E-SRPM)和跨层安全和资源感知路由协议(cross layer secure and resource-aware on demand routing, CSROR). E-SRPM 和 CSROR 都是通过采用文献[11]中的安全机制,在路由表中保存 2 跳邻居节点信息,记录邻居节点的不可靠值,通过对邻居节点不可靠值的判断来提供路由安全保护和选出最短的安全路径.

上述成果虽然能够为 HWMN 提供一定的路由安全保障,但还存在以下不足:1)缺乏对内部恶意节点的识别和管理,无法抵御内部攻击;2)缺乏提供隐私安全的保护;3)缺乏考虑路由过程中终端节点的参与和路由路径的能耗.

针对上述不足,本文将内部攻击的防御、节点的能量损耗和隐私安全的保护引入路由协议设计.通过建立和评估节点间的信任关系,实现对内部恶意节点的有效识别和管理,减少内部攻击发起的可能和由此导致的隐私信息的泄漏;同时,通过设计和实施新的隐私安全策略,实现了对节点访问隐私信息的限制和隐私信息在传输过程中的安全保障;最后,通过在路由建立过程中采用节点能量损耗评估模型,实现了安全路由协议的节能目标.

2　安全和攻击模型

2.1　安全模型

本文通过以下 2 种机制的协同工作来实现 HWMN 中的路由安全和隐私保护.

1) 预防机制.避免和减少攻击造成的危害.本文提出基于节点安全等级和安全类别的分级密钥管理协议(hierarchical key management protocol, HKMP),对节点的活动(即路由发现和数据传输)及节点对隐私信息的访问进行约束.HKMP 规定只有满足安全需求的节点才能参与路由发现和数据传输,有效地抵御了内部攻击,减少了隐私信息泄露的可能.此外,通过对不同类别的隐私信息采用不同的密钥,严格限制了节点对隐私信息的访问和获取,有效保护了隐私信息安全.

2) 响应机制.对攻击行为作出及时响应.本文提出动态信誉机制和恶意节点分类管理机制对恶意行为作出及时、准确地响应.动态信誉机制对节点行为进行动态评估,依据评估结果判断节点是否为恶意节点,能够及时、准确地发现节点的恶意行为.恶意节点分类管理机制对被识别出的恶意节点进行灵活的管理,依据行为的危害程度对节点作出惩罚或直接隔离网络(而不是直接隔离网络),延长了恶意行为记录在网络中的存在时间,减少了恶意节点参与路由转发的可能.

2.2　攻击模型

HWMN 面临的网络攻击主要分为 2 类:外部攻击和内部攻击[2,11-12].外部攻击能够通过传统的密码学方法和认证技术来有效解决;内部攻击的攻击者拥有合法的身份,能够获取各种密钥和授权信息,传统的密码学方法和认证技术无法有效地解决.

本文主要研究 HWMN 中的内部攻击,具体考虑以下 2 种攻击行为[2,11]:

1) 黑洞/灰洞攻击.黑洞攻击对截获的数据包进行篡改或丢弃所有的数据包;灰洞攻击则是在进行数据包转发的时候,以一定概率丢弃数据包.

2) 虫洞攻击.虫洞攻击旨在阻止正常的路由发现或通过在恶意节点间建立隧道来转移数据流,从而将恶意节点添加到路由路径中.一旦恶意节点包含加入到路由路径中,他们将丢弃所有或部分的数据包.

3　基于主观逻辑的动态信誉机制

3.1　动态信誉机制

传统静态信誉机制[13]存在以下不足:1)没有考虑信誉度随时间的变化,将上一次的评估结果作为当前的直接信誉度评估结果,缺乏动态性和实时性,无法体现节点最新的行为特点和及时更新信誉度.2)无法通过恶意节点最近的行为对节点进行及时重新评估及采取相应的措施(加重或减轻惩罚或允许节点重新加入网络),因此,无法实现对恶意节点的重新确认和灵活管理.

针对上述不足,本文在前期工作的基础上[14],提出了基于主观逻辑的动态信誉机制①.新的动态信誉机制中,节点信誉度的评估和节点间的信任关系不仅仅取决于当前的实时评估结果,也与距离上 1 次评估的时间间隔相关.

假设 $\omega_{t_i,x;y}^{\text{final}}(b_i,d_i,u_i,a_i)$ 为时刻 t_i 时节点 x 对节点 y 的综合信誉度评估结果,该结果保存在 x 的本地信誉度数据库中.$\omega_{t_n,x;y}^{\text{direct}}(b_n,d_n,u_n,a_n)$ 为时刻 t_n 时节点 x 对节点 y 的直接信誉度评估结果.考虑时间的影响,$\omega_{t_n,x;y}^{\text{direct}}$ 可以通过式(1)来计算:

$$\begin{cases} b_n = b_i \times \mathrm{e}^{-((b_i)^{-1}\Delta t)^{2k}}, \\ d_n = d_i \times \mathrm{e}^{-((d_i)^{-1}\Delta t)^{2k}}, \\ u_n = 1 - b_n - d_n, \\ a_n = a_i \times \mathrm{e}^{-((a_i)^{-1}\Delta t)^{2k}}, \end{cases} \tag{1}$$

其中,k ($k \geqslant 1$)为衰减率(信誉度随时间的变化率).$\Delta t = t_n - t_i$,当 $\Delta t \to \infty$ 时,$\mathrm{e}^{-((b)^{-1}\Delta t)^{2k}} \to 0$,使得 $b_n \to 0$,表明时间间隔越长之前的评估结果对现在的影响

① 由于篇幅限制,只介绍动态信誉机制的内容,主观逻辑及静态信誉机制的详细内容见文献[14]作者的前期工作.

越小. 时刻 t_n 直接信誉度的动态综合评估可以通过式(2)计算获得:

$$\begin{cases}\omega^{\text{direct}}_{\text{dynamic}(x;y)} = \eta_1 \times (b_i, d_i, u_i, a_i) + \\ \quad \eta_2 \times (b_n, d_n, u_n, a_n), \\ \eta_1 + \eta_2 = 1. \end{cases} \tag{2}$$

其中,η_1 和 η_2 代表节点关于时间对信誉度评估影响的重视程度,$\eta_1, \eta_2 \in [0,1]$,η_2 的值越大越重视时间的影响. 当 $E(\omega^{\text{direct}}_{\text{dynamic}(x;y)})$ 小于门限值时,节点将启动推荐信誉度和综合信誉度评估过程,获取邻居节点的推荐意见,并作出最后的评估和判断.

3.2 恶意节点分类和管理机制

新的动态信誉机制中还结合多级安全技术,提出了新的恶意节点分类和管理机制. 由于基于安全类别的处理方法和基于安全级别的方法相同,因此,本文只介绍基于安全级别的处理方法.

假设节点的安全等级为 1～5,每个等级的上下限分别为 TH_i^1 和 TH_i^2 ($TH_i^1 < TH_i^2, i=1,\cdots,5$). 当节点 x 完成了对节点 y 的综合信誉度评估,节点 x 将继续进行如下操作:

1) 将综合信誉度评估结果与每个安全级别的上下限比较,确定节点 y 的安全等级.

2) 根据节点 y 的安全等级判断节点 y 是否是恶意节点. 如果是,节点 x 将依据节点 y 的安全等级来决定是对节点 y 作出惩罚还是直接隔离.

由于不是武断地隔离所有的恶意节点,而是依据恶意节点的安全等级和安全类别采取惩罚或隔离措施,实现了对恶意节点的灵活管理,改善和提高了网络的容错性和可生存性.

4 分级密钥管理协议

为了保证传输过程中的路由安全和隐私安全,本文提出了新的分级密钥管理协议 HKMP. HKMP 使用 2 元组(RL,RC)来表示节点间的密钥对,RL 和 RC 分别表示节点的安全级别和安全类别. HKMP 通过可信密钥管理中心为每个安全级别分发独立的密钥池和初始密钥,并规定节点间只有 2 者的安全等级和安全类别都满足安全要求,才能够相互通信和获取信息,避免了拥有合法安全级别却没有合法权限的节点参与到路由过程中和获取隐私信息.

4.1 密钥的预分配

假设节点安全等级为 m,密钥池 SL 的定义如下:

$$SL = \{sl_1, sl_2, \cdots, sl_m\}, \tag{3}$$

其中,sl_j 为安全级别 j 的密钥池,包含 3 个部分:初始密钥 IK_j、子密钥集 RL_j 和 RC_j. RL_j 包含 $j-1$ 个安全级别密钥 sl_j^i ($1 \leqslant i < j-1$),用于与具有相同或更低安全级别的节点建立连接;RC_j 包含 n 个安全类别密钥 sc_j^p ($1 \leqslant p < n$),用于与具有相同安全级别,但是拥有不同安全类别的节点建立连接. 3 者的定义如式(4)所示:

$$\begin{cases} sl_j = \{IK_j, RL_j, RC_j\}, \\ RL_j = \{sl_j^{j-1}, sl_j^{j-2}, \cdots, sl_j^1\}, \\ RC_j = \{sc_j^1, sc_j^2, \cdots, sc_j^n\}. \end{cases} \tag{4}$$

RL_j 和 RC_j 可以通过 IK_j 来获得:

$$\begin{cases} RL_j = \{sl_j^i \mid sl_j^i = H(IK_j \parallel i)\} (1 \leqslant i \leqslant j-1), \\ RC_j = \{sc_j^p \mid sc_j^p = H(IK_j \parallel p)\} (1 \leqslant p \leqslant n). \end{cases} \tag{5}$$

4.2 密钥的生成

创建了 sl_j 之后,节点间按照下述方法建立密钥.

1) 节点 u 和 v 具有相同的安全级别 j,它们将通过以下方式计算它们之间的密钥:

① u 利用 1 个伪随机函数 f 生成 sl_j^u 和 sc_j^u:

$$\begin{cases} sl_j^u = f_{IK_j}(u), \\ sc_j^u = f_{IK_j}(u). \end{cases} \tag{6}$$

② u 发送请求消息给 v,并等待 v 的响应.

$$u \rightarrow *: u, j, \text{nonce}. \tag{7}$$

③ v 收到消息后,发现与 u 的安全级别相同,于是 v 计算 sc_j^v 并返回响应消息给 u.

$$\begin{cases} sc_j^v = f_{IK_j}(v), \\ v \rightarrow u: v, MAC(sl_j^v, sc_j^v, u \mid v), \text{ nonce}. \end{cases} \tag{8}$$

④ 如果 $sc_j^u = sc_j^v$,则 u 和 v 都能通过式(9)计算出它们之间的密钥:

$$sl_j^{uv} = f_{sl_j^v}(u) = f_{sl_j^u}(v). \tag{9}$$

2) 节点 u 和 v 属于不同的安全级别,u 的安全级别为 g,v 的安全级别为 h ($1 \leqslant g < h$),u 和 v 之间的密钥可以通过式(10)来获得:

$$\begin{aligned} sl_{gh}^{uv} &= f_{sl_{gh}^v}(u), \\ sl_{gh}^{v} &= f_{sl_h^g}(v). \end{aligned} \tag{10}$$

HKMP 中,假设 u 和 v 的安全级别分别为 g 和 h ($g < h$). v 的安全级别 h 大于 g,可以使用初始密钥 IK_h 和单向 Hash 函数 H 计算出 $sl_h^g = H(IK_h \parallel g)$,得到 sl_{gh}^v 和 sl_{gh}^{uv}. 而 u 的密钥池中没有 sl_h^g,所以无法得到 sl_{gh}^u 和 sl_{gh}^{uv}. 因此,即使攻击者俘获低安全级别的节点,但是由于无法获取更高安全级别节点的密钥,也就无法获取对方的隐私信息,从而实现了对隐私信息的安全保护.

5　节点能耗评估模型

在 HWMN 中,终端节点能够以自组织的方式构建终端网络并参与路由活动,但是,它们面临能量受限的问题.为了使得路由协议能够同时满足安全和节能的需求,本文使用成本效益分析模型[15-16]设计了新的节点能耗模型,对成功传输每个数据包所需要的能量进行分析,并将分析的结果用于选择最终的路由路径.

假设存在 N 个终端节点,每个节点的传输队列为 $M/M/1/K$ 排队系统,流量分布遵循速率为 λ 的泊松分布,e_{tx},e_{rx},e_{ov} 和 e_{id} 分别表示节点在传送、接收、监听和空闲状态下的能量需求.终端节点成功传输 1 个数据包所需要的总能耗 E 为

$$E = E^{su} + E^{co} + E^{bf} + E^{em}, \tag{11}$$

其中,E^{su} 是成功传输的能量损耗,E^{co} 是成功传输前的冲突造成的能量损耗,E^{bf} 是处于退避阶段的能量损耗,E^{em} 是在 2 个连续的传输之间不存在不确定数据包的情况下的能量损耗.

下面我们将分别介绍这 4 个组成部分的计算过程.

1) 我们通过式(12)来计算 E^{su}:

$$E^{su} = e_{tx} \times (T_L + T_H) + e_{rx} \times T_{ACK} + e_{id} \times T_{SIFS}. \tag{12}$$

2) 通过式(13)(14)来计算 E^{co}[15-16]:

$$E^{co} = (e_{tx} \times (T_L + T_H) + e_{id} \times (T_{SIFS} + T_{ACK} + T_{DIFS})) \times \varphi. \tag{13}$$

$$\begin{cases} \varphi = \sum_{j=0}^{\infty} j \times p^j \times (1-p) = p/1-p, \\ p = 1-(1-\tau)^{n-1}, \\ \tau = (1-P_0) \times \tau', \\ \tau' = \{2 \times (1-2 \times p)\} / \{(1-2 \times p) \times (W+1) + p \times W \times (1-(2 \times p)^m)\}, \end{cases} \tag{14}$$

其中,n 是 1 跳范围内的邻居节点数,W 是最小竞争窗口大小,m 是最大退避次数,P_0 是传输队列为空的概率,可以通过式(15)来计算:

$$\begin{cases} P_0 = 1 \Big/ \sum_{j=0}^{K} \left(\frac{\lambda}{\mu}\right)^j, \\ \mu = \frac{1}{E_S}, \end{cases} \tag{15}$$

其中,K 是缓冲区的大小,μ 是服务速率,它们可以计算得到[15-16]:

$$\begin{cases} E_S = E_A + E_B, \\ E_A = T_c \times \varphi + \sigma' \times \delta, \\ E_B = T_s, \\ T_c = T_s = T_L + T_H + T_{SIFS} + T_{ACK} + T_{DIFS} + 2\Delta, \end{cases} \tag{16}$$

$$\begin{cases} \sigma' = (1-P_t) \times \sigma + P_s \times T_s + (P_t - P_s) \times T_c, \\ \delta = \sum_{j=0}^{\infty} \sum_{h=0}^{j} \frac{W_h - 1}{2} \times p^j \times (1-p), \end{cases} \tag{17}$$

$$W_h = \begin{cases} 2^h \times W, & 0 \leqslant h \leqslant m', \\ 2^{m'} \times W, & m' < h \leqslant m, \end{cases} \tag{18}$$

其中,m' 是竞争窗口可以翻倍的最大次数,σ 是 1 个物理时间槽的长度,P_s 是在所有剩余的等待传输的节点中可以实现成功传输的概率,P_t 是在所有剩余的等待传输的节点中至少 1 个节点能够在 1 个逻辑时间槽内传输数据包的概率.P_s 和 P_t 可以通过式(19)来计算:

$$\begin{cases} P_t = 1-(1-\tau)^{n-1}, \\ P_s = (n-1) \times \tau \times (1-\tau)^{n-2}. \end{cases} \tag{19}$$

3) 如果信道被感知到是空闲的,退避计数器将在每个物理时间槽递减;否则,退避计数器将停止计数.因此:

$$E^{bf} = (e_{id} \times \sigma + e_{ov} \times (P_s \times T_s + (P_t - P_s) \times T_c)) \times \delta. \tag{20}$$

4) 此外:

$$\begin{cases} E^{em} = T^{em} \times (e_{id} \times (1-P_t) + e_{ov} \times P_t), \\ T^{em} = E_S \times \frac{P_0}{1-P_0}. \end{cases} \tag{21}$$

6　隐私感知安全路由协议

6.1　路由建立

RPASRP 的路由建立过程包括路由发现和路由响应 2 个子过程.

路由发现过程通过源节点构建路由请求消息 PREQ,并广播该消息给邻居节点来启动.假设 γ_1,γ_2($\gamma_1 < \gamma_2$,γ_1,$\gamma_2 \in [0.0, 1.0]$)为信誉度的门限值,具体的路由发现过程如下所述:

Step1. 源节点 y 向邻居节点广播 PREQ 消息,启动路由建立过程.

Step2. 邻居节点 x 收到 PREQ 消息后,采用动态信誉机制判断源节点 y 是否可信,具体步骤如下:

Step2.1. x 向本地信誉度数据库查询 y 的直接

信誉度 $\omega_{x;y}^{\text{direct}}$,并计算动态直接信誉度 $\omega_{\text{dynamic}(x;y)}^{\text{direct}}$.

Step2.2. 如果 $E(\omega_{\text{dynamic}(x;y)}^{\text{direct}})<\gamma_1$,则判断 y 为恶意节点;否则,判断 y 为可信节点.如果不存在 $\omega_{x;y}^{\text{direct}}$ 或 $\gamma_1<E(\omega_{\text{dynamic}(x;y)}^{\text{direct}})<\gamma_2$,则 x 启动下述信誉度查询过程.

Step2.2.1. x 广播查询消息给邻居节点,要求提供关于 y 的直接信誉度评估结果,并等待对方的回应,等待的时间长为 T.

Step2.2.2. 假设 x 和 y 的共同邻居节点 k 收到了查询消息,k 查询本地信誉度数据库,如果存在 $\omega_{k;y}^{\text{direct}}$ 且 $u_{k;y}^{\text{direct}}<1.0$,则 k 发送 $\omega_{k;y}^{\text{direct}}$ 给 x.

Step2.2.3. 经过时刻 T 后,x 将收到的所有推荐信息汇总,计算出 $\omega_{x;y}^{\text{recommend}}$ 和综合信誉度 $\omega_{x;y}^{\text{final}}$.

Step2.2.4. 经过时刻 T 后,x 将收到的所有推荐信息汇总,计算出 $\omega_{x;y}^{\text{recommend}}$,$\omega_{x;y}^{\text{rec}}$ 和综合信誉度 $\omega_{x;y}^{\text{final}}$.

Step3. 如果 y 是可信的,x 发送 Accept 消息给 y,并记录和 y 之间进行了 1 次良性交互;否则,x 发送 Refuse 消息,并记录进行了 1 次恶性交互.然后,x 执行恶意节点分类和管理机制,对 y 作出惩罚或直接隔离出网络.

Step4. y 收到 Accept 消息后,首先比较二者的安全级别.如果 y 的安全级别 g 高于 x 的 h,y 将拒绝 x 作为其下 1 跳中继节点;否则,y 将执行 Step2,Step3 来判断 x 是否是恶意节点.如果不是,并且 $g=h$,y 计算 2 者之间的密钥,并发送响应消息给 x.如果 $1\leqslant g<h$,则 y 发送响应消息给 x,由 x 来计算 2 者之间的密钥.

Step5. 反复执行 Step2,Step3,Step4,直到找到满足要求的路径.

Step6. 如果存在多条满足要求的路径,我们将通过式(22),找出最可靠的路径 L_{final}:

$$\begin{aligned} L_{\text{final}} &= \max(\varphi_{i1}\times\omega_{L(i)}+\varphi_{i2}\times SL_{L(i)}),\\ &\quad i=1,\cdots,n,\\ \text{s.t.}\quad &\varphi_{i1}+\varphi_{i2}=1,\\ &Th_1<E_{L(i)}<Th_2, \end{aligned}\tag{22}$$

其中,$L(s),(s=1,\cdots,n)$ 是满足要求的路径集合;Th_1 和 Th_2 是路径 $L(i)$ 的能量损耗 $E_{L(i)}$ 的门限值;$\omega_{L(i)}$ 和 $SL_{L(i)}$ 分别是 $L(i)$ 的信誉度和安全级别;φ_{i1} 和 φ_{i2} 是 $L(i)$ 的信誉度和安全级别的权重系数,通过式(23)来计算:

$$\begin{cases} \omega_{L(i)}=\min\left(\sum_{j=1}^{m}\omega_j^i/m,\ \min(\omega_j^i)\right),\\ SL_{L(i)}=\min(SL_j^i),\\ E_{L(i)}=m\times\max\left(\sum_{j=1}^{m}E_j^i/m,\max(E_j^i)\right), \end{cases}\tag{23}$$

其中,$N_j^i(N_j^i\in L(i),j=1,\cdots,m)$ 代表第 i 条路径 $L(i)$ 上的第 j 个节点;ω_j^i 和 SL_j^i 分别是 N_j^i 的信誉度和安全级别;E_j^i 是 N_j^i 的能量损耗.

路由响应过程在目标节点收到路由发现的消息后,由目标节点沿路由发现消息所经过的路径,返回 PREP 消息给源节点来启动.

6.2 路由维护

RPASRP 采用信道感知策略[17]来实现路由维护.假设 v_i,v_{i-1} 和 v_{i+1} 为路由路径上的节点,v_{i-1} 和 v_{i+1} 为 v_i 的上行和下行节点.具体路由维护过程如下:

1) v_i 定期执行上下行流量检测,检测 v_{i+1} 是否有丢包等恶意行为,同时通过测量 v_i 和 v_{i-1} 之间的链路丢包率来检测 v_{i-1} 的行为.

2) v_i 将检测结果与门限值比较,判断上下行节点是否为恶意节点.如果是,v_i 将返回 1 个路由维护信息给源节点.

3) 当源节点收到路由维护信息,它将重新启动路由发现过程,寻找其他安全的路径,并且,广播通知网络中的其他节点对恶意节点作出惩罚或将其隔离出网络.

7 仿真与性能分析

本文使用 OPNET[18]进行仿真实验和性能分析.仿真场景为 IEEE 802.11s 定义的 HWMN[7].仿真使用的部分参数如表 1 所示.仿真结果是通过 50 次仿真实验的平均数据.

Table 1 Simulation Parameters

表 1 仿真参数表

Parameters	Values
Traffic Type	CBR
Simulation Time/s	100
Packet Size/B	1 024
Data Rate, Basic Rate/Mbps	11, 1
Simulation Area/m^2	1 000
Number of Nodes	50
Buffer Size/packet	25
e_{tx}, e_{rx}, e_{ov}, e_{id}/W	1.65, 1.4, 1.4, 1.15
a_0, β, γ_1, γ_2, η_1, η_2	0.5, 0.5, 0.3, 0.6, 0.3, 0.7
(CWmin/CWmax)/B	16/512
(SIFS/DIFS)/μs	10/50
Propagation Delay, σ/μs	2, 20
T/ms	10

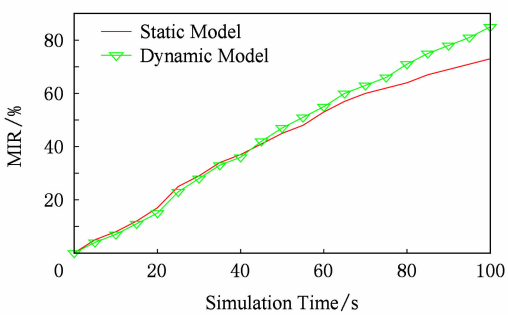
7.1　信誉机制性能分析

首先,我们比较动态和静态信誉机制在 3.2 节所述攻击下的恶意节点识别率和网络吞吐量.

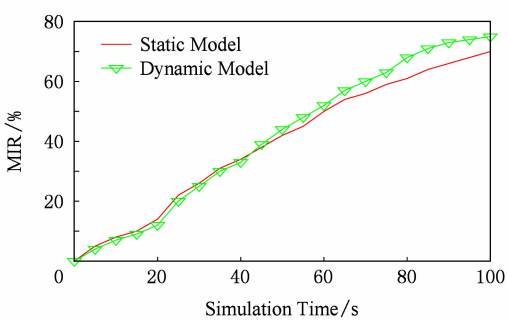
1) 恶意节点识别率

恶意节点识别率(malicious nodes' identification rate, MIR)体现了信誉机制防御内部攻击和保护隐私信息的能力. 提高 MIR,能够有效减少恶意节点参与路由建立和数据包转发的可能,从而减少隐私信息的泄露.

仿真结果如图 2 所示,从图 2 中可以看出 2 种机制的 MIR 都随时间的增加而增长. 然而,在 2 种攻击中,动态机制的 MIR 都高于静态机制. 在初始阶段,由于处于信任关系建立阶段,没有历史信息可以参考,2 种机制都依据节点的行为进行信誉度评估,因此它们的 MIR 很接近;随着时间的增长,信任关系建立完成,动态机制对信誉度评估的动态性克服了静态机制只依靠历史记录来识别恶意节点的缺点,能够更及时准确地评估节点的行为并作出反应,因此,其 MIR 性能更优.



(a) MIR under blackhole/grayhole attacks



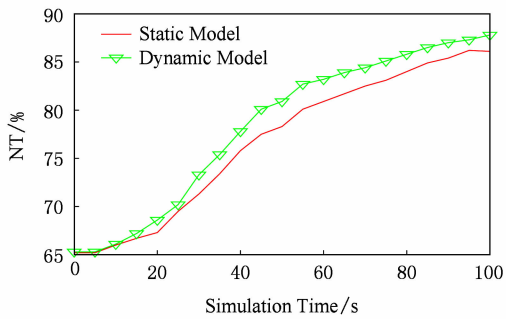
(b) MIR under wormhole attack

Fig. 2　MIR with different attacks.

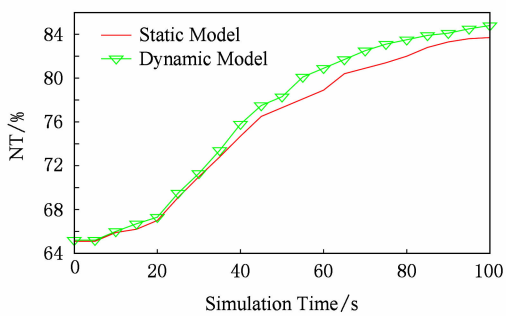
图 2　不同攻击下的恶意节点识别率

2) 网络吞吐量

2 种机制的网络吞吐量(network throughput, NT)的比较结果如图 3 所示,从图 3 中可以看出:①信誉机制能够有效提高吞吐量. 随着时间的增长,信誉机制的作用越来越大,恶意节点被识别出的可能性也逐渐增加,由恶意节点发起的内部攻击逐渐减少,从而导致吞吐量的逐渐提高. ②动态机制的吞吐量高于静态机制. 由于动态机制在节点安全等级和安全类别的划分和权限分配中采用灵活多样化的处理方式,并且对恶意节点采取了动态和灵活管理,从而有效地改善和提高了网络的容错性和生存性,使得更多节点能够参与数据包的转发,因此动态机制的吞吐量更高.



(a) NT under blackhole/grayhole attacks



(b) NT under wormhole attack

Fig. 3　NT with different attacks.

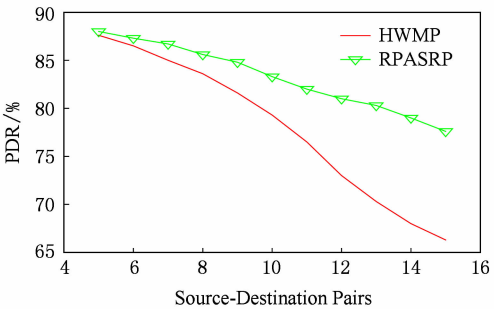
图 3　不同攻击下的网络吞吐量

7.2　路由协议性能分析

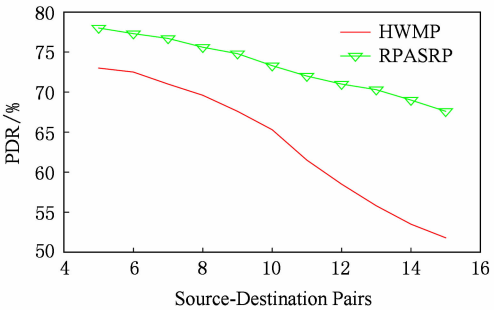
我们比较 RPASRP 和 HWMN 默认的混合无线网状网协议(hybrid wireless mesh protocol, HWMP)的分组传输率和端到端时延. 仿真实验中,将仿真场景细分为 2 个子场景:1)包含 10% 的恶意节点;2)包含的 30% 恶意节点.

首先,我们将比较 2 种协议的分组传输率(packet delivery ratio, PDR). 图 4(a)(b)分别为 2 个子场景下的仿真结果. 仿真结果表明:恶意节点的存在使得数据包在传输的过程中,可能由于遭受恶意攻击而被丢弃或不能到达目的节点,从而导致 PDR 的下降;同时,我们还发现在 2 个子场景中,RPASRP 的 PDR 下降的速度和幅度都小于 HWMP,原因在于:HWMP 协议中缺乏相应的恶意节点检测和管理机制,无法解决由于内部背叛的或被俘或的节点所做出的恶意丢包行为. 因此,随着节

点对的增加和恶意节点数量的增加,更多的恶意节点参与到数据转发和传输中,从而导致了 HWMP 的 PDR 的快速大幅度下降. 反之,RPASRP 针对 HWMP 的缺陷,提出了相关的路由安全保护机制,能够有效地、灵活地及动态地实现对恶意节点的识别和管理,阻止了大量恶意节点参与到数据转发和传输中,大大减小了 PDR 下降的速度和幅度.



(a) Packet delivery ratio with 10% malicious nodes



(b) Packet delivery ratio with 30% malicious nodes

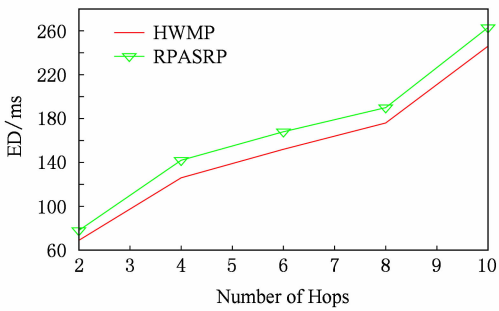
Fig. 4 Packet delivery rate with different percentage of malicious nodes.

图 4 不同比例恶意节点下的分组传输率

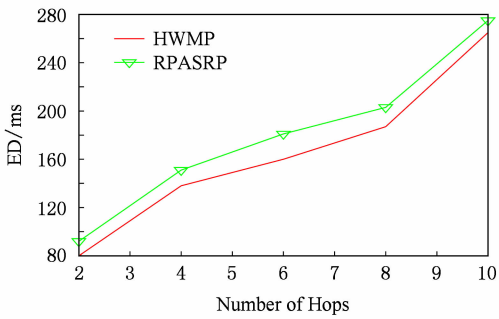
我们比较 2 种协议的端到端时延(end to end delay, ED). 仿真结果如图 5 所示:随着跳数的增加,2 种协议的 ED 也随之增加. 并且,在 2 个子场景中,RPASRP 的 ED 都高于 HWMP. 在流量负载较小、跳数较少的情况下,2 种协议的 ED 都小于 200 ms,随着流量负载的增大和跳数的增加,2 种协议的 ED 增加到 270 ms 左右. 由于 RPASRP 需要花费更多的时间用于实现保障路由和隐私安全的动态信誉机制等安全机制,因此 RPASRP 具有较高的 ED. 此外,恶意节点和恶意攻击行为的出现,使得 2 种协议都需要花费更多的时间用于路由发现和数据传输,因此,图 5(b)所示的子场景 2 下 2 种协议的 ED 都比子场景 1 下的高.

7.3 隐私安全性能分析

RPASRP 除了能够抵御内部攻击、提供路由安全保障,还能在以下 2 个过程中实现隐私安全保护.



(a) End to end delay with 10% malicious nodes



(b) End to end delay with 30% malicious nodes

Fig. 5 End to end delay with different percentage of malicious nodes.

图 5 不同比例恶意节点下的端到端时延

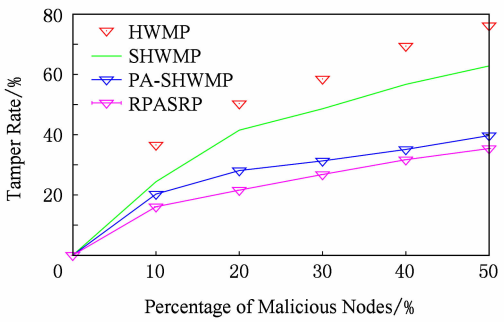
1) 路由发现和路径选择过程. RPASRP 将动态信誉机制与节点安全等级和安全类别相结合,确保了只有满足安全要求的节点才能参与路由发现和路径选择,减少了恶意节点加入到路由路径中的可能,从而降低了恶意节点通过发起内部攻击来获取隐私信息的可能. 同时,分级密钥管理协议的实施,也严格限制了节点对隐私信息的访问,进一步减少了隐私信息泄露的可能.

2) 数据传输和路由维护过程. 假设存在未被检测出的恶意节点,它们将在数据传输过程中发起攻击,导致大量数据包的丢失. RPASRP 通过路由维护机制,在攻击出现的时候,通过对上下行节点的监控来发现恶意节点,并通知源节点重新进行路由选择,从而及时有效地制止了恶意节点的攻击行为,减少了隐私信息的泄露.

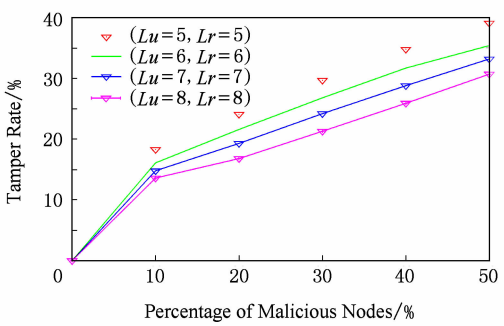
我们通过比较 HWMP,SHWMP[7]、隐私感知的安全混合无线 Mesh 网络路由协议(privacy aware secure hybrid wireless mesh protocol, PA-SHWMP)[14]和 RPASRP 的平均篡改率(即被篡改的数据包的比率)来验证 RPASRP 的隐私保护能力.

首先,我们比较 4 种协议的平均篡改率. 从图 6(a)可以看出,随着恶意节点比例的增加,4 种协议的平均篡改率也随之上升. 其中,HWMP 由于缺乏

相应的隐私保护措施,它的篡改率最高. SHWMP 虽然实现了对可修改字段的加密,但是,没有考虑内部节点的背叛或被俘获的可能,不能预防内部攻击. 因此,在出现背叛或被俘获节点时,其用于保护隐私安全的加密手段就失去了作用. PA-SHWMP 中采取了节点安全等级划分、隐私信息安全分类和字段的分类加密这些机制,能够有效抵御内部攻击和实现隐私安全保护,因此,它的平均篡改率较低. RPASRP 由于具有比 PA-SHWMP 更细颗粒度的节点安全等级、安全类别和权限的分配及更严格的隐私信息的访问限制,因此,它的平均篡改率最低.



(a) Tamper rate among four protocols



(b) Tamper rate with different security level and security class

Fig. 6　Tamper rate with different percentage of malicious nodes.

图 6　不同比例恶意节点下的篡改率

我们通过比较 RPASRP 中不同安全等级数和安全类别数的平均篡改率来进一步说明 RPASRP 的隐私保护能力. 仿真结果如图 6(b)所示. 其中,Lu 代表节点安全等级的级数(即不同的用户数),Lr 代表节点的安全类别的类别数(即相同的用户可以分配的角色的数目). 从图 6(b)可以看出,由于恶意节点数目的增加,导致动态信誉机制的识别有效性和准确性下降,一些新的恶意节点或行为危害度较轻的恶意节点仍旧能够参与到路由发现和数据转发的过程中,因此,不同级数/类别数的平均篡改率也随之上升;然而,从图 6(b)可以看出,安全等级的级数或安全类别的类别数越大,其平均篡改率越低. 原因在于:等级/类别划分的颗粒度越小,节点参与路由发现和数据转发的安全需求颗粒度也就越小,访问隐私信息的安全要求也就越严格. 该结果说明 RPASRP 能够实现对于隐私信息的细颗粒度的安全保障,增强了隐私保护的能力;同时,通过对隐私信息的细颗粒度划分,还可以进一步的预防重要隐私信息的泄露.

7.4　路由能耗性能分析

最后,我们比较 HWMP,PA-SHWMP,RPASRP 的路由能量损耗. 仿真结果如图 7 所示,随着源目节点对数目和跳数的增加,3 种协议的路由能量损耗也随之增加. 然而,由于 RPASRP 在最后的路径选择过程中综合考虑了节点的能量损耗,因此,即使在具有相同跳数的情况下,RPASRP 的路由能量损耗仍旧低于 HWMP 和 PA-SHWMP,具有良好的节能性能,能够有效提高终端节点的能源使用效率.

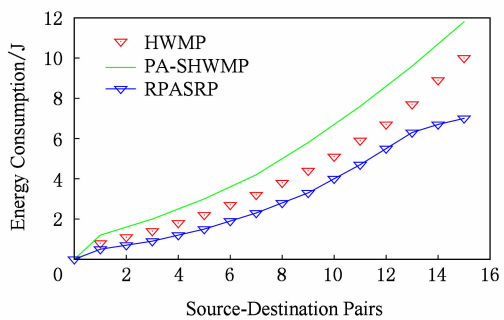


Fig. 7　Routing energy consumption with different number of source-destination pairs.

图 7　不同节点对数下的路由能量损耗

8　结　　论

本文针对 HWMN 中的路由安全、隐私安全和路由能量损耗问题展开研究,提出了基于动态信誉机制的隐私感知安全路由协议 RPASRP. RPASRP 提出了新的动态信誉机制和恶意节点分类和管理机制,考虑了时效性对信誉度评估的影响,增强了评估的动态性和准确性,并实现了对恶意节点的灵活管理,增强了网络的容错能力和生存能力. 此外,RPASRP 还提出了新的分级密钥管理协议,保证了路由和隐私信息在传输过程中的安全. 最后,RPASRP 将能量损耗问题引入路由协议,提出节点能耗评估模型和基于节点能耗的路径选择机制,使得 RPASRP 能够同时满足安全和节能的需求. 仿真结果和分析表明,RPASRP 协议能够有效地抵御内部攻击,实现隐私保护,并减少路由过程中的能量损耗.

参 考 文 献

[1] Akyildiz I F, Wang X, Wang W. Wireless mesh networks: A survey [J]. Computer Networks, 2005, 47(4): 445-487

[2] Ben-Othman J, Claude J P, Benitez Y I S. A novel mechanism to secure internal attacks in HWMP routing protocol [C] //Proc of the 2012 Int Conf on Communications (ICC). Piscataway, NJ: IEEE, 2012: 162-166

[3] Khan S, Alrajeh N A, Loo K K. Secure route selection in wireless mesh networks [J]. Computer Networks, 2012, 56 (2): 491-503

[4] Khan S, Loo J. Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks [J]. Wireless Personal Communications, 2012, 62(1): 201-214

[5] Li Xiaoqing, Li Hui, Yang Kai, et al. A secure routing protocol based on D-S evidence theory in ad hoc networks [J]. Journal of Computer Research and Development, 2011, 48(8): 1406-1413 (in Chinese)
(李小青, 李晖, 杨凯, 等. 一种基于 DS 证据理论的 Ad Hoc 网络安全路由协议[J]. 计算机研究与发展, 2011, 48(8): 1406-1413)

[6] Wu Yue, Li Jianhua, Lin Chuang. Survey of security and trust in opportunistic networks [J]. Journal of Computer Research and Development, 2013, 50 (2): 278 - 290 (in Chinese)
(吴越, 李建华, 林闯. 机会网络中的安全与信任技术研究进展[J]. 计算机研究与发展, 2013, 50(2): 278-290)

[7] Islam M S, Hamid M A, Hong C S. SHWMP: A secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks [G] //Transactions on Computational Science Ⅵ. Berlin: Springer, 2009: 95-114

[8] Ren Kui, Yu Shucheng, Lou Wenjing, et al. PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks [J]. IEEE Trans on Parallel and Distributed Systems, 2010, 21(2): 203-215

[9] Sen J. An efficient and user privacy-preserving routing protocol for wireless mesh networks [J]. International Journal Scalable Computing: Practice and Experience, 2011, 11(4): 345-358

[10] Sen J. Security and Privacy Issues in Wireless Mesh Networks: A Survey [M]. Berlin: Springer, 2013: 189-272

[11] Khan S, Loo K K, Mast N, et al. SRPM: Secure routing protocol for IEEE 802.11 infrastructure based wireless mesh networks [J]. Journal of Network and Systems Management, 2010, 18(2): 190-209

[12] Shivlal M, Kumar S U. Performance analysis of secure wireless mesh networks [J]. Research Journal of Recent Sciences, 2012,1(3): 80-85

[13] Yang Kai, Ma Jianfeng, Yang Chao. Novel trusted routing in wireless mesh networks [J]. Journal of Applied Sciences, 2011, 29(3): 221-227 (in Chinese)
(杨凯, 马建峰, 杨超. 一种新的无线网状网可信路由[J]. 应用科学学报, 2011, 29(3): 221-227)

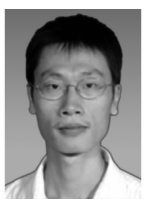
[14] Lin Hui, Ma Jianfeng, Hu Jia, et al. PA-SHWMP: A privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks [J]. EURASIP Journal on Wireless Communications and Networking, 2012, 69 (1): 1-16

[15] Hu Jia, Min Geyong, Woodward M E. Performance analysis of the TXOP burst transmission scheme in single-hop ad hoc networks with unbalanced stations [J]. Computer Communications, 2011, 34(13): 1593-1603

[16] Hu Jia, Min Geyong, Jia Weijia, et al. Comprehensive QoS analysis of enhanced distributed channel access in wireless local area networks [J]. Information Sciences, 2012, 214 (1): 20-34

[17] Shila D M, Cheng Y, Anjali T. Mitigating selective forwarding attacks with a channel-aware approach in WMNs [J]. IEEE Trans on Wireless Communications, 2010, 9(5): 1661-1675

[18] Chen Min. OPNET Network Simulation [M]. Beijing: Tsinghua University Press, 2004



Lin Hui, born in 1977. PhD, associate professor and master supervisor in the School of Mathethmatics and Computer Science, Fujian Normal University. Member of China Computer Federation. His main research interests include wireless and mobile computing systems, information and network security(linhui@fjnu.edu.cn).

Tian Youliang, born in 1982. PhD, associate professor and master supervisor in the College of Science, Guizhou University. Member of China Computer Federation and ACM. His main research interests include algorithm game theory, cryptography and information security.

Xu Li, born in 1970. PhD, professor and PhD supervisor in the School of Mathethmatis and Computer Science, Fujian Normal University. Member of IEEE and ACM, senior member of China Computer Federation. His main research interests include wireless network and communication, network and information security, etc(xuli@fjnu.edu.cn).

Hu Jia, born in 1981. PhD and lecturer in Department of Mathematics and Computer Science, Liverpool Hope University. His research interests include performance modelling and analysis, network protocols and algorithms, next generation networks, cross-layer optimization, network security, and resource management(jiahu9@gmail.com).