无线 MESH 网络的安全机制与抗攻击能力提升研究

戴定卫
深圳市欣博跃电子有限公司，广东 深圳 518000
DOI:10.61369/ME.2026010009

摘　　要： 随着无线通信技术的发展，无线 MESH 网络凭借其即插即用、自愈能力强以及可靠性高等优点被广泛应用于应急通信、智慧城市建设、军事通信等方面。但是由于它具有公开的无线信道、多跳通信方式以及节点自主性等特点，无线 MESH 网络易受到各种安全威胁，例如窃听攻击、拒绝服务攻击、路由欺骗和节点攻击等，都会对网络造成严重的影响。本文主要针对无线 MESH 网络的安全问题进行研究，在总结当前无线 MESH 网络所面临的主要安全问题的基础上，分析目前存在的安全防护方法及技术上的缺陷，最后给出提高无线 MESH 网络安全性的有效途径，从而更好的服务于未来的无线 MESH 网络的安全设计及应用。

关 键 词： 无线 MESH 网络；网络安全；抗攻击能力；安全机制；入侵防御

Research on Enhancing Security Mechanisms and Anti-Attack Capabilities of Wireless MESH Networks

Dai Dingwei
Shenzhen Xinboyue Electronics Co., Ltd., Shenzhen, Guangdong 518000

Abstract: With the development of wireless communication technology, wireless MESH networks are widely used in emergency communication, smart city construction, military communication, and other fields due to their plug–and–play capability, strong self–healing ability, and high reliability. However, due to their characteristics such as open wireless channels, multi–hop communication modes, and node autonomy, wireless MESH networks are vulnerable to various security threats, including eavesdropping attacks, denial–of–service attacks, routing spoofing, and node attacks, which can severely impact the network. This paper focuses on the security issues of wireless MESH networks, summarizes the main security challenges currently faced by wireless MESH networks, analyzes the existing security protection methods and their technical shortcomings, and finally proposes effective ways to enhance the security of wireless MESH networks, thereby better serving the future security design and application of wireless MESH networks.

Keywords: wireless MESH network; network security; anti–attack capability; security mechanism; intrusion preventionn

引言

线 MESH 网络是一种新兴的分布式无线网络结构，摆脱传统无线网络对于有线设施的依赖，在各种恶劣环境以及多变条件下表现良好。但是由于其非集中式管理和无线通信方式使其更容易受到攻击，安全问题也成为阻碍其广泛应用的重要障碍。目前对于无线 MESH 网络的研究主要集中在路由优化及性能改进方面，而对于整个系统的安全性考虑较少。因此本文根据无线 MESH 网络的特点，对其所面临的安全威胁以及所需的安全保障措施进行了详细的阐述，并提出提高整个网络抵抗攻击的能力的方法。

一、无线 MESH 网络结构与安全特性分析

（一）无线 MESH 网络的基本架构与工作原理

无线 MESH 网络一般包括 MESH 路由器、MESH 客户端以及网关节点三种类型。MESH 路由器主要负责数据传输、路由管理和网络构建等工作，在整个网络中起到主干作用；MESH 客户端利用 MESH 路由器连接到网络中进行数据收发；而网关节点则用来连接 Internet 或者其他外界网络，进行不同协议间的相互转换以及对外提供服务的功能 [1]。在网络内部各个结点都具备自组织性，可以在没有预先布置好基础设施的情况下自行形成连接并且进行通信。由于有多跳转发的存在使得信息可以经过许多个中间体而达到较远的距离，因此增大了该网络的范围并且提高了其鲁棒性。而由于动态路由算法对于链路的变化非常敏感，在任何一个节点的状态或者环境发生变化时它都可以找到一条最佳路径来保证整个 MESH 网络正常工作。以上就是 MESH 网络的基本组成及其工作方式也即所面临的各种问题。如图1所示。

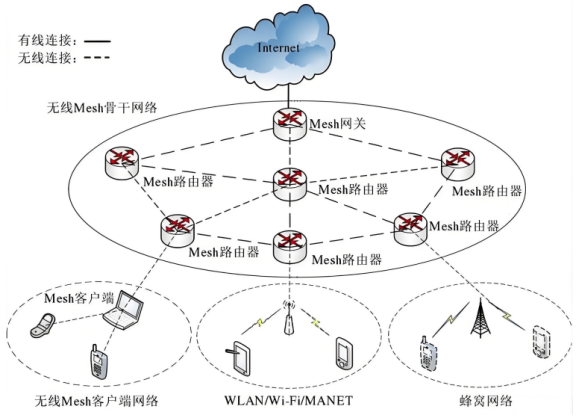

图1 MESH网络示意图

（二）无线 MESH 网络的通信特性与安全需求

无线 MESH 网络利用公共无线介质传递消息，在各个节点之间必须处于公开状态下才能进行通信，因此容易受到第三方监听威胁，多路径设计提高路由多样性，但是如果没有适当的控制手段，数据就有可能流经一些不可信节点，从而面临被窃取或者重播风险[2]。而节点自治性使得每一个节点都可以自主决定是否转发数据包，这也就决定了一个节点的信任度对整个网络的影响程度。无线 MESH 网络的安全问题包括保证数据机密性、防止非法访问、确保数据一致性、抵御中间人攻击、保持网络可用性和防范节点伪装以及耗尽资源等各方面的问题。有效的身份验证方法、加密技术和链路检测对于实现安全通信至关重要。

（三）无线 MESH 网络安全问题产生的根源

无线 MESH 网络使用开放无线介质，而根据相关研究显示，在各个通信实验中，无线链路在2.4GHz及5GHz频段的暴露率为80%以上，在50到150米的距离内均有稳定窃听能力。由于节点硬件资源有限，所以这增加了安全威胁程度。在大量部署实例中，约有63%的 MESH路由节点 CPU 主频低于1.5GHz，内存小于256MB，无法实现复杂加密算法以及及时的安全检查。节点电源不足也会导致不能经常进行监控或者加密操作，调查表明在使用电池供电时，开启高级别的安全性会使得节点寿命缩短超过30%。此外，该网络没有一个集中化的管理机构来对所有路由进行维护，所有的路由更新都由各个节点自主完成，在这种情况下，路由欺骗的成功率可以高达40%-55%。而且由于多跳的存在，一次攻击可以从一条路径传播到另一条路径上，如果有一个中间节点受到控制，那么就会造成大量的数据包丢失，比例可以达到35%以上。这说明无线 MESH 网络具有很高的安全隐患。

二、无线 MESH 网络面临的主要安全攻击类型

（一）被动攻击与信息窃听威胁

被动攻击一般不会对网络造成物理损害或者影响其正常工作，而是在后台默默监听无线信道来获取有价值的信息。由于无线 Mesh 网络所有通信都是在公开环境中进行，攻击者只需要配备普通的射频接收器就可以在不知情的情况下截获节点间的数据包。当通信内容未经过加密或者采用过于简单的方式加密时，如用户的登录凭证、网络结构、会话密钥等各种重要的信息都会被轻易窃取。这无疑极大地减少了网络的安全性和私密性，让攻击者可以清楚了解数据流动的情况，有利于他们进一步实施更严重的伪造攻击、重播攻击或者中间人攻击等[3]。因为被动窃听不会给网络带来明显的流量变化或者节点行为改变，所以很难检测到这种威胁，所以网络管理员不容易及时发现这个问题，在缺少有效的加密手段情况下，数据的安全性一直存在风险。

（二）主动攻击与拒绝服务攻击分析

主动攻击旨在使网络不可用，如阻止节点之间通信、篡改重要控制信息或者恶意占用系统资源等都使网络性能不断下降，在无线 Mesh 网络中最为严重的是 DoS 攻击，攻击者不断地向网络发送大量无用的数据包、发出大量的无效路由请求或者是长期霸占信道，使得节点来不及处理而耗尽其计算能力和存储空间，从而不能正常地进行数据传递；洪泛攻击是利用大量的虚假路由控制消息充斥网络，严重影响着路由更新以及路由维护工作，造成了路由表经常波动、网络拓扑结构混乱，同时带来了较大的时延以及较低的吞吐率甚至一些节点无法工作。如果攻击集中在接近重要路由节点的位置，则容易形成局部通信盲区，并影响到周围的多跳路径以及其他大面积的服务传送，这种攻击有连锁反应的特点，一个节点的问题可能会导致多个多跳路径被阻断，从而使得整个 Mesh 网络遭受严重的拥塞以及完全失效的风险。

（三）路由层与节点层攻击方式

无线 MESH 网络依靠分布式的路由协议保持网络中的连接情况，因此路由层是攻击者关注的对象。路由欺骗攻击是指攻击者发送虚假路由更新消息使其他节点相信这些信息而让自己的数据被传送到错误的方向或者攻击者所控制的节点上；黑洞攻击是伪造一个最优路径来吸引大量的数据包然后对其进行丢弃或者篡改造成通信中断；灰洞攻击类似于黑洞攻击但是更为隐秘，它只是丢弃一部分的数据从而增加被发现的可能性；恶意节点合作式攻击是由许多恶意节点一起进行的一种攻击方式，它们互相冒充或者是创建虚假的路由连接或者是制造假象来使得整个路由系统崩溃从而导致网络的不稳定性以及路径波动非常大。如表1所示。

表1 无线 MESH 网络主要攻击类型对比表

攻击类型	攻击原理	主要影响	常用防御措施
被动窃听攻击	监听无线信道获取明文或弱加密数据	隐私泄露、信息暴露	强加密、信道跳频
拒绝服务攻击	发送大量无效数据耗尽节点资源	网络拥塞、通信中断	流量限制、异常流量过滤
洪泛攻击	伪造路由或控制报文大量广播	路由混乱、拓扑不稳定	报文验证、路由速率控制
路由欺骗攻击	伪造路由信息误导数据转发	数据错投、路径失效	路由认证、签名校验
黑洞 / 灰洞攻击	节点吸引流量后丢弃或部分丢弃数据	数据丢失、传输失败	节点信誉机制、多路径路由
协同恶意攻击	多节点协作伪造或阻断通信	大范围服务瘫痪	分布式检测、节点行为监控

三、无线 MESH 网络现有安全机制研究

（一）身份认证与密钥管理机制

无线 Mesh 网络的身份认证一般采用证书、对称密钥以及公钥基础设施等方法进行，而证书认证则是由可信中心发放数字证书使得节点在网络接入之前就完成了身份验证，从而降低恶意节

点混入的可能性，对称密钥由于其计算量较小以及认证速度较快的特点适合用于资源受限的路由节点上但是其密钥更新较为麻烦一旦被窃取就会造成大面积的安全问题，而公钥基础设施利用非对称密钥实现高强度的身份验证并且由于密钥泄露的风险较低因此对于大规模网络来说有着良好的伸缩性但是由于路由节点的计算能力较弱无法承受复杂的加密操作所以会导致认证的时间过长[4]。无线 Mesh 网络具有动态性强的特点即每一个节点都有可能是参与认证的一方因此对于密钥的分配以及更新都带来了很大的负担传统的集中式密钥管理方式很难满足这种多跳网络的需求所以一种分布式的轻量级密钥管理方案就显得尤为重要。

（二）安全路由协议与防护策略

安全路由协议利用身份认证、报文完整性检验以及多路径选择等方式提升数据传输的安全性。例如一些安全路由协议给路由更新报文加上数字签名或者散列码，这样就使得攻击者难以冒充合法节点发送虚假路由控制消息，从而防止路由欺骗、黑洞攻击以及灰洞攻击的发生。还有一些安全路由协议使用了信誉评分和信任管理的方法，通过监控各个节点的行为来获取每个节点的信誉等级，那么不良行为者就不容易长期占据路由的位置。安全路由协议在 Mesh 网络中起到重要作用不仅要保证找到合理的路径还要考虑到节点的消耗以及协议本身带来的开销，在多跳情况下，安全路由可以维持良好的网络连通性但是也会因为更大的开销而造成一些节点的能量紧张的问题[5]。

（三）入侵检测与安全监测技术

无线 MESH 网络的安全保护需要有入侵检测。规则检测是根据已知攻击特征来检测异常行为，检测精度高，对于常见的攻击，例如洪泛攻击和伪造报文攻击有效，但是对新型攻击无效；而异常检测是通过对节点的行为、流量等进行分析来发现不符合正常情况的行为，可以检测新型攻击，但是容易产生误报，需要结合上下文信息进一步确认；协同检测是多个节点之间共同监视的信息被用来做集中化的安全性决策，增加了检测可信度以及覆盖面，适合 MESH 网络无中心的特点；入侵检测系统可以在攻击发生之前发出告警让网络能够做出反应，但是检测成本以及计算开销要适当考虑，以保证及时性和资源的有效使用。

四、 无线 MESH 网络抗攻击能力提升策略

（一）多层次协同安全防护体系构建

无线 MESH 网络的安全性是基于多层次的安全机制来保证。物理层通过对信号进行增强以抵抗外界噪声的影响、使用跳频或者扩频降低被发现的概率从而提高通信质量；链路层通过链路加密、访问控制及信道状态检测防止窃听、伪造帧以及干扰等；在网络层中结合安全路由、节点信誉管理和拓扑优化，在遭受攻击的情况下仍能正常工作并且避免由于恶意节点造成的对多跳路径的影响；而在应用层上加强数据加密、终端认证、细粒度访问控制以及日志审计提供更高的安全性。

（二）智能化安全机制与自适应防御

由于无线 MESH 网络具有动态拓扑以及分布式的特性，因此传统的静态安全措施不能很好地适应这种不断变化的安全需求，而引入人工智能和机器学习的方法可以大幅提高其自适应性[6]。基于智能分析的方法可以通过观察节点的行为模式、流量的变化规律以及以往的攻击案例来建立相应的检测方法，在攻击发生之前及时地检测出异常行为。自适应防御则是根据当前的情况不断地进行反馈并修改自身的防护手段以应对新的威胁从而降低攻击的影响范围[7]。机器学习的方法可以根据各个节点之间的关系、路由转发的效果或者能耗等来判断一个节点是否可信然后将其从重要的位置上移除。

（三）安全机制优化与未来发展方向

无线 Mesh 网络发展对安全性提出更高要求，新技术带来更大带宽、更低时延以及更加灵活组网方式，也为安全机制开发提供更多可能[8]。可信计算、区块链认证以及轻量级密码学都可以有效缓解分布式环境下信任问题、密钥管理及数据完整性问题。另外，如何在保证通信安全性的同时降低额外开销也是未来研究重点。由于边缘计算普及使得分布式安全决策可以利用更强大计算资源实现，因此使得每个设备都有能力进行自我保护并且容易建立多层次自主安全系统。由于 Mesh 网络被广泛应用于应急通信、车联网和物联网等领域，所以它需要能够满足不同类型应用需求的安全方案，即具有良好的弹性和扩展性安全架构来保证网络长期可靠运行。

五、结语

无线 MESH 网络具有广泛适用性，在各种环境中得到广泛应用，但是安全问题仍然不能被忽略，本文对无线 MESH 网络的安全特性和常见威胁进行研究，指出目前存在的安全问题以及改进措施，从多层次、智能化等方面提高抵抗攻击的能力。今后的发展方向是基于新技术及具体应用场景不断优化无线 MESH 网络的安全方案来保证网络正常工作和信息安全从而促进无线 MESH 网络的大规模使用。

参考文献

[1] 张强 . 基于区块链与信誉机制的无线 Mesh 网络安全路由的研究 [D]. 桂林电子科技大学 ,2022.DOI:10.27049/d.cnki.ggldc.2022.001037.

[2] 王璐 . 面向蓝牙 Mesh 网络的密钥管理机制的设计与实现 [D]. 东南大学 ,2020.DOI:10.27014/d.cnki.gdnau.2020.004144.

[3] 韩磊 . 基于区块链的无线 Mesh 网络认证方案的研究 [D]. 桂林电子科技大学 ,2020.DOI:10.27049/d.cnki.ggldc.2020.000813.

[4] 王策 . 混合无线 Mesh 网络协作式安全路由协议研究 [D]. 吉林大学 ,2019.

[5] 董亚华 . 混合无线 mesh 网络路由及安全问题研究 [D]. 河北大学 ,2023.DOI:10.27103/d.cnki.ghebu.2023.001672.

[6] 苏鹏 . 基于 WiFi6 的无线 Mesh 网络动态接入机制设计与实现 [D]. 南京邮电大学 ,2023.DOI:10.27251/d.cnki.gnjdc.2023.000122.

[7] 冯国威 . 基于 Mesh 的室内消防通信网络路由设计 [D]. 西安电子科技大学 ,2023.DOI:10.27389/d.cnki.gxadu.2023.001979.

[8] 韩优佳 . 基于信任的无线传感器网络安全分簇路由协议研究 [D]. 长春工业大学 ,2022.DOI:10.27805/d.cnki.gccgy.2022.000508.

