解决方案：mesh网的安全研究及解决方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/207/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_207192.htm WMN（WirelessMeshNetwork）是一种动态的自组织、自配置的网络。网络中的各节点自动建立成一个Adhoc网络并保持一种网状连接。WMN具有前期投入低、系统容量大、维护简单、可靠性高等许多优点。802.11 mesh网是一种802.11和mesh相结合的组网结构，它使用一组网状的无线路由器相连来提供一定区域的无线覆盖。由于802.11 mesh网的一些特点，这种网络也带来了一些不同于传统802.11网络的一些新的安全挑战。1、802.11mesh网概述 1.1 802.11mesh网的组网结构 部署传统无线网络时，人们总是苦于难以寻找到合适的有线接入点，尤其在空旷、缺乏铜线/光纤等有线资源的室外环境中，问题更加明显。WMN的出现在很大程度上解决了这一问题：传统WLAN中，每一个AP都需要通过有线接入点连接到有线局域网；而802.11mesh网络由一组呈网状分布的无线路由器组成，无线路由器必须实现两个功能：用户接入（即传统802.11无线局域网AP的功能）和无线中继（即转发数据给另一无线路由器）。如图1所示，只需要设置部分无线路由器通过有线接入点连接到宽带骨干网就足够了，至于无线路由器之间则采用点对点方式通过无线中继链路互联，而在无线路由器对用户终端提供802.11连接。这大大减少了对有线资源的需求，极大地便利了无线网络的部署。 图1 802.11mesh网 1.2 802.11mesh网的关键技术 当前，业界的802.11mesh网体系结构不尽相同，主要区别在于无线中继的方式和无线中继链路路

由选择的方法。无线中继手段，业界主要的分歧在于采用Multi-Band、Multi-radio方式还是采用Single-Band、Single-radio方式。如果用户接入和无线中继工作于同一频段，如使用工作于2.4GHz的802.11b作为用户接入，同时使用同样工作于2.4GHz的802.11g作无线中继，就是一种Single-Band、Single-radio方式。反之，用户接入和无线中继工作于不同频段，如使用工作于2.4GHz的802.11b/g作为用户接入，同时使用工作于5.8GHz的802.11a作无线中继，则是一种典型的Multi-Band、Multi-radio方式，采用Multi-radio方式至少可以将接入部分和无线中继部分从频率上分开，使得两者互不干扰，能在一定程度上提升性能。 而在路由算法上，沿用有线网络路由协议还是开发专用的无线mesh路由协议也是两种截然不同的技术路线。Mesh路由的目的是为了寻找最优或相对最优的回传路径。在无线网络中，网络性能同发送成功概率息息相关。在WMN中，一个好的路由算法必须兼顾减少路由跳数以及降低某条链路上包错误概率。在这个意义上，传统的有线路由协议并不适合于无线mesh路由，因为它通常无法考虑一条无线链路上包错误概率。因此，单从性能角度来考察，必须开发适用于无线环境的mesh路由协议。 2、802.11mesh网的安全 2.1 802.11mesh网的安全挑战 Mesh网和802.11无线局域网相比多跳通信是一个主要的安全挑战。众所周知无线通信很容易受到被动攻击（如窃听），以及主动攻击（如信息篡改，DOS攻击）。而这些安全隐患在多跳的mesh网中将被进一步放大。（1）在802.11无线局域网中每个用户端都和AP相连，所以有利于管理员的管理。但是由于802.11mesh网是一个多跳网络，所以将所有的安全管理都集

中一端的无线网关将延缓网络对攻击的检测和应对，这将无疑会给攻击者带来好处。（2）由于无线路由器距离Internet接入点有近有远，远离Internet接入点的节点有可能获得很小的带宽，所以设计合理的协议来保证节点间公平是很重要的。然而对公平性的保护也带来了新的挑战。（3）在有线网络中路由器一般会得到妥善的保护，所以对有线网络中的路由器的攻击不是那么方便，然而不同于有线网的路由器无线路由器一般都在室外分布，比如安放在楼顶或安放在路灯上。所以无线路由器得不到很好的物理保护。这很容易造成攻击者对无线路由器的攻击，比如修改路由器中的信息，窃取路由器中用于认证的对称密钥或公私钥对，或者用非法的无线路由器替换合法的。（4）由于无线路由器得不到很好的物理保护，攻击者可以潜入网络伪装成合法的节点，发布错误的路由信息。所以必须设计安全的路由协议以对抗针对路由协议的攻击。 2.2 802.11mesh网的安全解决方案 目前802.11mesh网的安全方案主要是Tropos的TroposMetroMesh方案和Nortel的方案。Tropos Metro Mesh方案，采用了多层安全架构，对客户机提供WEP、WPA保护；对无线路由器间的数据采用64/128 bit WEP或128bit AES加密；同时使用VPN来增强整体的安全性。 链路层的保护是无线网络安全机制的第一步，但是单独的链路层保护不能提供对敏感数据的保护。TroposMetroMesh使用了一系列方法来保护链路层的安全：（1）使用WEP通过用加密所有的帧来提供网络接入控制和安全数据传输。但是WEP被证明易受被动攻击，如果单独使用不能提供充分的安全性。（2）WPA是Wi-Fi联盟最新的安全标准，它使用更强的密码体制。WPA利用EAP和RADIUS提供

更强的认证，它还提供了基于802.1x的端口接入控制。（3）使用128bitAES加密所有终端用户在mesh网中多跳传输的数据直到它们到达一个有线网关。（4）使用MAC地址接入控制列表：接入点通过设置可接入名单和黑名单来进接入控制。但是因为物理地址可以被修改所以基于MAC地址的接入控制只能当作多层安全体制中的一部分。（5）抑制网络名（ESSID）：接入点允许管理员有选择的抑制网络可用性的广播，这样可以使非法的节点不能发现接入点，除非他使用探测工具。（6）多网络名（ESSID）：使用多接入点标示可以灵活适应有不同无限设备和安全性的用户组。在三、四层Tropos使用VPN来实现网络接入控制和保护数据传输。在无线路由器上使用流量过滤来加强VPN提供的安全。使用128bit AES加密PWRP路由协议传输的节点身份和路由选择路径信息。 管理信息的加密：作为网关的无线路由器从与它相关联的节点收集管理信息并发送到管理服务器，并使用AES加密这些流量。所有的无线路由器可以使用基于Web的配置来进行配置和监控，所有的配置信息使用httpS进行保护，这样网络管理者可以安全的配置和监控每一个无线路由器。 Nortel在安全方面也别具特色。每个无线路由器间均建立经过加密的IPSec隧道，以便安全地传送所有用户的数据业务、内部信令处理和管理信息，也就是说数据在无线路由器之间的传送都处于IPSec保护之下。不过网关并不涉及用户的认证工作。对于具有WPA（802.11i）功能的用户而言，无线路由器会将用户的认证信息经过IPSec加密隧道“ 透明地 ”传送到网络中心的RADIUS认证服务器进行合法性认证。通过认证后，无线路由器与用户间的传输资料就会以WPA/802.11i加密

算法加密，用户的传输资料将经由IPSec加密隧道，在无线路由器之间传送直到网关。另外，无线路由器不仅支持多种用户WPA：EAP-TLS、EAP-TTLS、EAP-PEAP；还在无线路由器间采用以WPA为基础的认证功能，对新加入网络的无线路由器进行认证，防止非法无线路由器接入。并使用基于WPA的加密功能，保证邻近无线路由器间传送的路由和通信控制协议的安全。 3、结束语 802.11mesh网将传统WLAN与mesh网结合起来增强了网络的覆盖能力以及可靠性。此外它在移动漫游等方面与传统WLAN相比较同样也有着明显的优势。2004年1月，IEEE802.11Working Group正式专门成立了网格研究组（Mesh Study Group），同年3月又成立了网格任务组（Mesh Task Group）。目的就是将mesh网的优点写进802.11协议中去。但是目前对802.11 mesh网的研究还处于起步阶段，还有很多需要解决的问题，尤其是对其安全研究的工作还很少。Tropos和Nortel安全方案都颇具特色，将无线侧的数据完全处于加密防护下，代表了无线802.11 mesh网络安全方案的发展趋势。 