Securing Wireless Mesh Networks

Now found in domestic, commercial, industrial, military, and healthcare applications, wireless networks are becoming ubiquitous. Wireless mesh networks (WMNs) combine the robustness and performance of conventional infrastructure networks with the large service area and self-organizing and self-healing properties of mobile ad hoc networks. In this article, the authors consider the problem of ensuring security in WMNs, introduce the IEEE 802.11s draft standard, and discuss the open security threats faced at the network and data-link layers.

Steve Glass, Marius Portmann, and Vallipuram Muthukkumarasamy
Queensland Research Lab, NICTA

Wireless mesh networks (WMNs) offer improved utility and lower infrastructure costs than conventional wireless networks because, like mobile ad hoc networks manets, they use multihop routing. This routing strategy extends the wireless service area and enables the network's self-healing and self-organizing properties. A WMN is distinct from manets in that it uses multiple radios and relies on a high-speed back-haul network — itself, often wireless — that optimizes network performance and provides gateways to the wired Internet and other wireless services. (Ian Akyildiz, Xudong Wang, and Weilin Wang have surveyed the existing literature on WMNs elsewhere.[1])

Early adopters of wireless mesh technology include community networks, which can provide low-cost Internet access to whole neighborhoods by buying inexpensive wireless mesh routers from companies such as Meraki. WMNs are also appealing in the developing world, as evidenced by the One Laptop per Child project's XO laptop, which is designed for educational use and implements a wireless mesh network using hardware and software that conforms to the IEEE 802.11 standard but has extensions to support wireless mesh networking. With millions of units in projected XO sales, IEEE 802.11 use for mesh networking is set to expand rapidly.

The IEEE formed the 802.11 Task Group "s" (TGs) in 2004 to prepare a standards amendment to meet the requirements for WMNs. The standards amendment, which will be known as

 1089-7801/08/$25.00

802.11s, is expected to be ratified in the last quarter of 2009, and efforts are already under way to integrate it into the GNU/Linux kernel. (An overview of the 802.11s architecture and concepts is available elsewhere.[2])When used in sensitive applications, WMNs need robust security protocols to ensure secure operation. The protocols should ensure the confidentiality, integrity, and authenticity of network traffic and preserve the availability of communications. A more comprehensive set of requirements might also address the problems of intrusion detection and location privacy.

As Figure 1 illustrates, security threats are present at all levels of the protocol stack, so security is a high priority within TGs. The draft amendment builds on the successful security protocols of the base standard and extends them so that they may be used in a WMN environment. In this article, we consider the challenges to WMN security at the data-link or MAC layer and the network layer.

Layer	Threats
Application	Logic errors, buffer overflows, privilege escalation
Transport	DNS spoofing, session hijacking, traffic injection
Network	Black/gray/worm holes, misrouting, rushing attacks
Data-link	Traffic flooding, virtual jamming, man-in-the-middle
Physical	Collision jamming, device tampering

Figure 1. Wireless Security Risks: Security threats are present at all layers of the wireless mesh network stack.

WMN MAC-Layer Security

A secure MAC layer is responsible for ensuring that a mesh network carries traffic only for authorized stations, thus preventing attacks by unauthorized ones. The following sections describe the requirements for a secure MAC as well as the 802.11s MAC-layer extensions that address them.

Availability

In the context of wireless networks, availability refers to the network services' survivability in the face of denial-of-service attacks. Availability is one of the most important properties for a wireless network; it's also one of the most difficult to ensure, which is a serious problem in 802.11 networks because jamming attacks are easy to mount but almost impossible to prevent. Given that an attacker can always resort to a jamming attack, IEEE 802.11 doesn't address availability concerns. Alternatively, the self-healing property in 802.11s WMNs — a property shared with manets — lets the WMN route traffic around jammed areas automatically. The WMN itself has another possible response because traffic might be routed to a different radio that uses a channel that the adversary isn't jamming. Although the adversary might also jam that channel, it does increase the work required for doing so.

Fairness

In a mesh network, the MAC must ensure that no station is starved of bandwidth. Ensuring *fairness* includes two distinct aspects: access to the radio channel and access for traffic forwarded through a given station. The former is the MAC layer's responsibility, and the latter falls to the routing or path-selection protocols.

802.11 defines several coordination functions (CFs) to provide contention-based and contention-free access to the wireless channel. The contention-based mechanisms allows collisions in transmission to occur and use an exponential back-off that favors stations that place the network under heavy load. Adversaries can exploit this inherent unfairness via traffic-flooding or MAC-layer attacks to deliberately starve other stations of bandwidth. 802.11s partly addresses the fairness problem by requiring the standard contention-based *enhanced distributed channel access* (EDCA) — a QoS-aware CF. That said, using EDCA in a WMN can set the stage for potential performance problems in the presence of hidden terminals. Such hidden terminals are within the radio range of the receiver but not of each other and so can cause interference at the receiver should they broadcast simultaneously. To counter this possibility, the standard defines an optional *mesh deterministic access* (MDA) CF that permits congestion-aware, contention-based, and contention-free access for WMNs. Contention-free access lets a station reserve exclusive access to the radio channel - preventing interference from hidden terminals. The risks associated with contention-free access are that a rogue station can continuously request bandwidth in order to prevent legitimate stations from communicating.

Authentication

Authentication allows one station to prove its identity to another. In conventional 802.11 networks, the problem of authentication and key distribution is explicitly outside the specification's scope. It assumes the existence of an enrollment mechanism that ties a user identity to an encryption key that can be used to establish credentials. Two basic approaches are available for authenticating within WMNs:

- *Preshared key* (PSK) approaches use passphrases or other key material provided to each station in advance.
- *Public key* (certificate-based) approaches use private keys to authenticate each station's identity.

PSK is simple and efficient, but it's flawed in that a single passphrase is often shared among all stations in the network. Knowledge of the passphrase is sufficient for decrypting any session or masquerading as any other station. Perhaps most serious is that attackers can defeat the 802.11 PSK using dictionary attacks, and several open-source tools, such as coWPAtty http://www.churchofwi.org/, can automate that attack process. In light of this, 802.11s prohibits the use of 802.11 PSK mode and implements a new mechanism known as MKD-PSK. This requires a unique 256-bit PSK for each station, which is shared only with a trusted third party known as the *mesh key distributor* (MKD). This eliminates the principal risks of the original PSK approach but requires the creation and distribution of unique PSKs for each mesh station.

Public-key-based approaches are extremely flexible and use certificates to verify station identities. Yet, this flexibility comes at a cost of increased complexity. From the WMN perspective, the main drawback is that all stations must be able to authenticate the certificates they receive. Unfortunately, a station joining the WMN for the first time will be unable to contact the certificate authority (CA) to check a certificate's revocation status until after it has authenticated itself.

Authentication and Access-Control Protocols

802.11 uses the 802.1X port-based access-control mechanism to manage authentication exchange and initiate the four-way handshake used for key establishment. The authentication exchange includes three parties: the supplicant seeking to be authenticated, the authenticator to which the association is being established, and the authentication server (AS) that's responsible for verifying the identities. 802.1X is very effective in conventional infrastructure environments, but it has shortcomings when used for WMNs. In the former, a single IEEE 802.1X exchange takes place between the supplicant station seeking to join the network and the access point, which is the authenticator. When used in a WMN, 802.1X requires that

- both stations must make two prior, complete IEEE 802.1X authentication exchanges to establish mutual authentication;
- both stations implement the supplicant and authenticator state machines, given that both roles must be performed;
- each station have access to the AS; and
- one station access the AS via the other, as-yet untrusted, station.

This approach is complex and time-consuming, and it negatively impacts the WMN's self-organizing property. Significant interest thus exists in alternative authentication protocols for mesh access. The dual wireless authentication protocol (DWAP) protocol,[3] for example, is an efficient alternative that substantially reduces the overhead associated with 802.1X. During the drafting of the standard, TGs considered another protocol, known as Comminus, that's designed specifically for the WMN environment.[4] Comminus is an efficient, lightweight, peer-based authentication protocol based on the secure key-exchange mechanism (SKEME) key exchange and management protocol. In contrast to 802.1X, Comminus doesn't distinguish between the roles played by the parties being authenticated and uses authentication frames rather than data frames to conduct its exchange. Some loss of generality occurs because Comminus supports only certificate or PSK modes, - although the latter mode is vulnerable to a dictionary attack. Although it is an interesting protocol, it does not support the extensible suite of authentication protocol EAP authentication types that's possible in 802.1X and is unlikely to make it into the standard.

Risks from Compromised Stations

A nasty problem for WMNs is the lack of physical security for network stations, which might be widely distributed geographically. An adversary might be able to physically capture a station, which presents risks not frequently experienced with an infrastructure network. Naouel Ben-Salem and Jean-Pierre Hubaux describe four key threats arising from the lack of physical security:[5]

- removal of network stations;
- inspection of stations to, for example, recover key material, routing tables, or traffic transiting the station;
- modification of a station's internal state; and
- cloning and deployment of compromised stations.

All but the first of these threats are particularly serious in that they expose the network to hostile attack. The latter two raise the possibility of byzantine attacks at a later stage. At this time, effective solutions to these problems remain open research problems.

Path Selection and Routing Security

Hybrid Wireless Mesh Protocol

802.11s is unusual in that the MAC layer is responsible for ensuring that a frame reaches its final destination across multiple hops and multiple potential paths. In manents and other WMNs, this role is usually performed by the routing protocol at the network layer. In 802.11s, Hybrid Wireless Mesh Protocol (HWMP) performs path selection at the MAC layer, and the protocol forwards frames at this layer. Because HWMP is a MAC layer protocol, it uses MAC addresses and not IP addresses; otherwise, it employs the same process as routing at the network layer. We can configure an 802.11s WMN to use either HWMP or a conventional network-layer routing protocol.

HWMP is a hybrid protocol in that it combines both proactive and reactive approaches to path selection. If a "root node" exists, HWMP uses proactive routing to find and maintain a route to it. Root nodes are special and will usually represent what 802.11 denotes as *mesh portals* (MPs) — mesh stations that serve as gateways to non-802.11 networks. Proactively maintaining a path to a root node is, therefore, an optimization for one of the most likely traffic destinations. For all other stations, the protocol uses reactive or on-demand path discovery exclusively. Reactive path discovery uses protocol primitives and rules from the ad hoc on-demand distance vector (AODV) routing protocol.[9] You can find an introduction to the 802.11s HWMP path selection protocol elsewhere.[10]

Routing Attacks

Attacks on the path selection and routing protocols can impact availability across large parts of the network. A hostile adversary can subvert the protocol by either

- attacking the route discovery mechanism by injecting, modifying, or misdirecting the route request (PREQ/RREQ), route reply (PREP/RREP), and route error (PERR/RERR) messages to affect the routing metrics, introduce gratuitous detours, attempt to create routing loops, or overflow routing tables; or
- forwarding attacks in which a station agrees to join a path but fails to route traffic in accordance with the protocol by dropping, delaying, or failing to forward traffic fairly.

To address these risks, researchers have proposed several secure routing protocols that use cryptography-based approaches to prevent attacks. (A survey of such protocols is available elsewhere.[11]) Using cryptography allows stations to authenticate the routing messages. The Authenticated Routing for Ad Hoc Networks (ARAN) protocol uses digital signatures to sign a message's contents at each hop.[12] Using public-key cryptography in this way is expensive, however, so researchers have sought other approaches. One common alternative is to use hash chains as introduced in the Secure Ad Hoc On-Demand Distance Vector (SEAD) protocol.[13] Hash chains are efficient and guarantee authenticity and integrity similar to digital signatures but at a lower cost.

Rushing Attacks

Rushing attacks subvert the route-discovery process to increase the likelihood that the hostile station is included in a given route. The attacker quickly forwards route request messages to ensure that duplicate requests arriving later from other stations will be suppressed.[14] The purpose of this attack is to increase the likelihood that the adversary's station is included in a given route. The defense against this attack has two parts: a secure neighbor discovery protocol and a modification to the routing protocol's

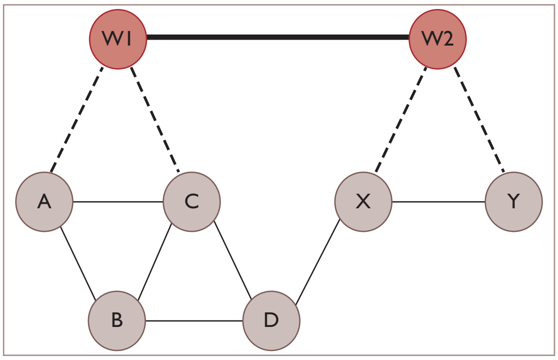

Figure 2. An example wormhole attack. The connection between stations W1 and W2 creates a "wormhole" in the WMN topology analogous to the wormholes of theoretical physics.

route-discovery logic. At present, these aren't integrated into popular WMN routing protocols. This attack remains a potential threat, especially when the WMN isn't using higher-layer end-to-end security protocols.

Gray Holes and Black Holes

A black hole is a station that advertises its willingness to take part in a route but forwards no traffic. A gray hole is a more difficult to detect variety that conditionally decides on which traffic it will forward. One key property of gray and black holes is that they must attract traffic through themselves to be effective. Gray or black hole attacks might alter route replies or use a rushing attack to improve their routing metrics and become the preferred route for network traffic.

Wormholes

Wormhole attacks can be severely problematic. With such attacks, the hostile adversary doesn't need to control any legitimate stations but still poses a significant outsider threat to the WMN's routing integrity. The wormhole attack forms a tunnel connecting different parts of the network, thus tricking stations adjacent to one end of the wormhole into believing that they're neighbors with stations at the other end. At first sight, a wormhole appears beneficial because it optimizes traffic flow across the mesh. The threat is that it also permits an adversary to conduct active traffic analysis and large-scale denial-of-service attacks.

Figure 2 shows an example wormhole attack in which the hostile adversary has two stations linked to each other via a high-speed data link. The stations are located within radio range of the WMN, and traffic overheard by one end of the wormhole is relayed to the other where it's then rebroadcast and similarly in the reverse direction.

In this example, station A would appear to have B, C, X, and Y as its direct neighbors, whereas Y would presume it has A, C, and X for its direct neighbours. Station B would conclude that it has three two-hop routes to station X, but only the route B -> D -> X avoids the adversary.

The threat posed by wormhole attacks is severe, and researchers have proposed several means of combating this threat. In essence such approaches seek to verify the authenticity of the transmission itself as well as the authenticity of the information actually exchanged.

Distance bounding protocols. Distance-bounding protocols seek to set an upper bound on the distance between legitimate parties by using precise timing of a cryptographic challenge/response. One such distance-bounding protocol is the secure tracking of node encounters (SECTOR) mutual authentication with distance-bounding (MAD) protocol, which we can use as a defense against wormhole and more general impersonation attacks.[15] MAD relies on measuring the round-trip times of a bit-commitment protocol and also unfortunately requires special hardware support for the distance-bounding protocol.

Yih Chin Hu and colleagues' paper, which first discussed wormhole attacks, also suggested using packet leashes to defend against them.[16] Packet leashes require either trustworthy geographical data or precisely synchronized clocks to restrict a packet's travel within a defined geographical area. As with Sector, the requirement for special hardware support limits this solution's appeal.

Neighbour verification. Turgay Korkmaz also considers the wormhole problem, but he uses time-of-flight and signal-power models as part of a neighbor-verification protocol (NVP).[17] NVP uses timing and power information to authenticate the exchanges. Unlike the secure verification protocol suggested to defend against rushing attacks, the NVP protocol isn't cryptgraphically secure. It is, nevertheless, a potential obstacle to hostile adversaries.

Jakob Eriksson advocates the TrueLink protocol[18] as an alternative approach. TrueLink isn't intended to be a true distance-bounding protocol, but stations can use it to establish the authenticity of neighboring stations. The protocol has two phases. First, stations exchange request-to-send (RTS) and clear-to-send (CTS) packets containing nonces - randomly-generated numbers. The timing requirements in this exchange are such that wormholes can't relay the RTS/CTS packets. Stations then use these nonces to answer non-time-critical periodic authentication challenges to prove that the RTS/CTS nonces are original which they do by sending signed messages authenticating themselves as the originator of their nonce value. Among the advantages of this approach are that it requires only minor changes to the MAC protocol and that it can work with standard hardware.

Reputation-Based Defenses

Reputation-based approaches such as the watchdog/pathrater protocol[19] offer a novel approach to detecting misbehaving stations (including routing unfairness and gray and black holes): they rely on neighbors to monitor each other and avoid paths via stations that don't behave properly. Unfortunately, such reputation-based approaches have limited applicability in WMNs because many stations employ multiple radios. A station could thus forward traffic using radio channels that its neighbors can't hear or monitor.

Security Verification

How can we prove that 802.11s is secure? The proposed standards amendment's security builds on the 802.11 committee's experience with TGi, which defined the TKIP and AES/CCMP protocols. Considerable attention has been paid to ensuring the security of any amendments. Doug Kuhlman and his colleagues developed a formal proof of security for the draft 802.11s specification[6] that uses Protocol Composition Logic (PCL) to demonstrate that the draft protocol is secure.

Security flaws are present not just in the WMN's design, but also in both its implementation and operation. Bugs in the implementation are a major source of security flaws. In one study, device drivers had error rates three times higher than other kernel code and rates as much as seven times higher for some classes of errors.[7] Security flaws are already evident in wireless device drivers, as we can see from notable security compromises of flawed wireless device drivers. Provably secure implementations will require changes in both the operating system device driver architectures and software-development practices.

Finally, some security problems come from insecure operational practices. Common misconfigurations, such as the use of self-signed certificates for authentication, can render well-designed protocols ineffective. We can verify secure operational practices by periodically using penetration-testing toolkits.

The benefits of using a WMN are substantial in terms of improved utility, availability, and reliability, but considerable challenges remain to securing real-world WMNs.

Securing the MAC layer can prevent unauthorized access to the WMN. The IEEE 802.11s amendment promises to be a major step forward in this respect by adapting the successful security protocols of the base standard to the WMN environment. These mechanisms rely on the presence of either the mesh key distributors (MKDs) or authentication servers (ASs) to authenticate new stations, and these servers must be available during mesh formation. Alternative authentication protocols that are lightweight and do not place restrictions on mesh formation remain an area for future work. The experience of the Comminus protocol shows this is possible but underscores the importance of rigorous validation.

The security risks to path selection are already familiar from the routing layer protocols used by manets. A variety of secure routing protocols such as ARAN and SEAD have been implemented to address these threats. A key challenge will be their adaptation to the WMN environment. New metrics and security designs will be needed to account for the WMN environment where the use of multiple radios changes some of the basic assumptions.

Finally, secure designs need to be matched by secure implementations. The use of model-checking techniques can identify security problems in the design of the security protocols. Employing secure implementation techniques and careful auditing can eliminate many problems before the protocol implementations enter live use. New techniques for implementing device-drivers can reduce the impact when problems occur. One particularly promising approach is to compartmentalize the drivers so they run with only the minimum necessary privileges outside of the main body of the operating system kernel.

Acknowledgments
NICTA is funded by the Australian Government as represented by the Department of Broadband Communications, and the Digital Economy, the Australian Research Council through the ICT Centre of Excellence program, and the Queensland government.

References

1. I.F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," *Computer Networks and ISDN Systems*, vol. 47, no. 4, 2005, pp. 445–487.
2. G.R. Hiertz et al., "Principles of IEEE 802.11s," *Proc. 16th Int'l Conf. Computer Comm. and Networks* (ICCCN 07), IEEE CS Press, 2007, pp. 1002–1007.
3. X. Zheng et al., "A Dual Authentication Protocol for IEEE 802.11 wireless LANs," *Proc. 2nd Int'l Symp. Wireless Comm. Systems*, IEEE CS Press, 2005, pp. 565–569.
4. D. Harkins and C. Kuhtz, *Secure Mesh Formation*, tech. report 802.11-06/1092r2, IEEE, 2006.
5. N.B. Salem and J.-P. Hubaux, "Securing Wireless Mesh Networks," *Wireless Comm.*, vol. 13, no. 2, 2006, pp. 50–55.
6. D. Kuhlman et al., *A Proof of Security of a Mesh Security Architecture*, tech. report 802.11-07/2436r0, IEEE Press, 2007; https://mentor.ieee.org/802.11/public-file/07/11-07-2436-00-000s-a-proof-of-security-of-a-mesh-security-architecture.doc.
7. A. Chou et al., "An Empirical Study of Operating System Errors," *ACM Operating Systems Rev.*, vol. 35, 2001, pp. 73–88.
8. Q. Lu, *Vulnerability of Wireless Routing Protocols*, tech. report, Univ. of Massachusetts, Amherst, Dec. 2002; www.nvc.vt.edu/ceege/qifeng/lukelu_files/Vulnerability_Qifeng%20Lu.pdf.
9. C.E. Perkins and E.M. Royer, "Ad-Hoc On-Demand Distance Vector Routing,": *Proc. 2nd IEEE Workshop on Mobile Computer Systems and Applications* (WMCSA 99), IEEE CS Press, 1999, pp. 90–100.
10. M. Bahr, Proposed routing for IEEE 802.11s WLAN mesh networks. Proc. 2nd annual international workshop on wireless internet (WICON 06), ACM Press, 2006, p. 5.
11. Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security & Privacy*, vol. 2, no. 3, 2004, pp. 28–39.
12. K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," *Proc. 10th IEEE Int'l Conf. Network Protocols*, IEEE CS Press, 2002, pp. 78–89.
13. Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," *4th IEEE Workshop on Mobile Computing Systems and Applications* (WMCSA 02), pages 3–13, June 2002.
14. Y.-C. Hu, A. Perrig, and D.B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," *Proc. 2003 ACM Workshop on Wireless Security*, ACM Press, 2003, pp. 30–40.
15. S. apkun, L. Buttyán, and J.-P. Hubaux, SECTOR: Secure Tracking of Node Encounters in Multihop Wireless Networks. Proc. 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM Press, 2003, pp. 21–32.
16. Y.-C. Hu, A. Perrig, and D.B. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE J. Selected Areas in Comm.*, vol. 24, no. 2, Feb. 2006, pp.370–380.
17. T. Korkmaz, "Verifying Physical Presence of Neighbors Against Replay-Based Attacks in Wireless Ad Hoc Networks, *Proc. Int'l Conf. Information Technology: Coding and Computing* (ITCC 05), IEEE CS Press, vol. 2, 2005, pp. 704–709.
18. J. Eriksson, S.V. Krishnamurthy, and M. Faloutsos, "Truelink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks, *Proc. 14th Ann. IEEE Conf. Network Protocols* (ICNP 06), IEEE Computer Society 2006, pp. 75–84.
19. S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. 6th Ann. Int'l Conf. Mobile Computing and Networking* (MobiCon 00), ACM Press, 2000, pp. 255–265.

Steve Glass is a research engineer at Queensland Research Lab, NICTA. His research interests include security in wireless mesh networks, intrusion detection and prevention systems, and public-safety communications. Glass has MSc in Computing from the Open University. Contact him at stephen.glass@nicta.com.au.

Marius Portmann is a senior lecturer at the University of Queensland, and a researcher at Queensland Research Lab, NICTA. His research interests include Pervasive Computing, Wireless Mesh Networks, P2P Computing and Network Security. Portmann has a PhD in Electrical Engineering from the Swiss Federal Institute of Technology (ETH), Zurich. He is a member of the IEEE and can be contacted at marius@ieee.org.

Vallipuram Muthukkumarasamy is a senior lecturer in the School of Information and Communication Technology, Griffith University. His research interests include Security in Wireless Networks, Intrusion Detection and Prevention Systems, Sensor Network Security, Information Assurance in e-Government Models, Adaptive Equalisation. Muthukkumarasamy has a PhD in Communications from University of Cambridge. He is a member of the IEEE. Contact him at v.muthu@griffith.edu.au.