International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Distinctiveness Governing Mobile Mesh Networks

[1] **M.SREENANDAN REDDY**, [2] **Mrs.B.NAGALAKSHMI**

1M.Tech Student, Department of Computer Science and Engineering, GATES Institute of Technology, Gooty, Andhra Pradesh, India.

2 Associate Professor in Department of Computer Science and Engineering, GATES Institute of Technology, Gooty, Andhra Pradesh, India.

Abstract—Multihop wireless mesh networks (WMNs) are finding ever-growing acceptance as a viable and effective solution to ubiquitous broadband Internet access. This paper addresses the security of WMNs, which is a key impediment to wide-scale deployment of WMNs, but thus far receives little attention. We first thoroughly identify the unique security requirements of WMNs for the first time in the literature. We then propose ARSA, an attack-resilient security architecture for WMNs. In contrast to a conventional cellular-like solution, ARSA eliminates the need for establishing bilateral roaming agreements and having real-time interactions between potentially numerous WMN operators. With ARSA in place, each user is no longer bound to any specific network operator, as he or she ought to do in current cellular networks. Instead, he or she acquires a universal pass from a third-party broker whereby to realize seamless roaming across WMN domains administrated by different operators. ARSA supports efficient mutual authentication and key agreement both between a user and a serving WMN domain and between users served by the same WMN domain. In addition, ARSA is designed to be resilient to a wide range of attacks. We also discuss other important issues such as incontestable billing.

Index Terms—Authentication, denial-of-service (DoS), key agreement, roaming, security, wireless mesh networks (WMNs).

I. INTRODUCTION

MULTIHOP wireless mesh networks (WMNs) are increasingly recognized as ideal solutions to ubiquitous last-mile high-speed Internet access. A typical WMN has a layered structure, as shown in Fig. 1. The first layer consists of access points (APs) which are high-speed wired Internet entry points. At the second layer, stationary mesh routers form a multihop backbone via long-range high-speed wireless techniques such as WiMAX [1]. The wireless backbone connects to wired APs at some mesh routers through high-speed wireless links. It provides multihop wireless backhaul

between wired APs and mesh clients (i.e., end users) at the lowest layer.1 Mesh clients, while at rest or in motion, can assess the network either by a direct wireless link to a nearby mesh router or by a chain of other clients to a mesh router out of reach. WMNs represent a unique marriage of

the ubiquitous coverage of wide-area cellular networks with the ease and the speed of local-area Wi-Fi networks. Other

notable advantages of WMNs include low deployment costs, self-configuration and self-maintenance, good scalability, high robustness, and so on [2]. Consequently, WMNs have sparkled a surge of research, development, and standardization activities, of which we refer to [2] for a comprehensive survey. Security is one of the main barriers to wide-scale deployment of WMNs, but has gained little attention so far. The necessity for security in large-scale WMNs can be best illustrated by the following example. Suppose David wishes to retrieve some important documents from his corporate network back in Miami via a local WMN in Philadelphia, where he is on a business stay. On the one hand, the serving WMN has to corroborate the identity of David to avert fraudulent use of network resources; on the other hand, David might as well want to authenticate the serving WMN to prevent an attacker from impersonating a legitimate WMN to obtain confidential information from him. Other security concerns may include the location privacy of David, passive eavesdropping, denial-of-service (DoS) attacks, and so forth. The security of nomadic users and the serving wireless networks has been studied extensively in the past. Elegant solutions are available in the contexts of Global System for Mobile Communications (GSM) [3], Personal Communication Systems (PCSs) [4], Universal Mobile Telecommunication System (UMTS) [5], and Mobile IP networks , among others. Despite their differences in specifics, these schemes all depend on a home/foreign-domain model. Specifically, each user has a home network domain, where he2 is registered on a long-term basis and account information is maintained. Each time the user roams into a foreign network domain, his home domain is contacted for his credentials to authenticate him. Subsequently, the foreign domain reports the amount of service assessed by the user to his home domain which, in turn, pays the foreign domain and charges the user an amount commensurate with his usage. We argue that such solutions are less suitable for future large-scale WMNs due to at least the following reasons. First, a bilateral service level agreement (SLA) has to be set up between each pair of network operators to permit user roaming between them. Establishing such SLAs may be a relatively easy task in cellular networks, where the operators are comparatively limited in number. Due to the easy-deployment nature of WMNs, however, the future large-scale WMNs are expected to comprise numerous WMN domains, each administrated by an independent operator [2]. Unlike a cellular operator often of a nationwide or larger scale, a WMN operator may be on a community, section, metro, or larger scale. Consequently, the number of WMN operators will be much larger than that of cellular operators. This renders it less feasible to establish pair wise bilateral SLAs among them. Second, the above solutions all involve a potentially time-consuming and expensive execution of an authentication protocol among a user, his home domain and the foreign domain. As the user base grows large, the overall network authentication signaling overhead would be significant. In addition, in view of the high-speed wireless link, the authentication latency may be unacceptable for some short-lived data applications. Assume, for example, that a mesh client connects to a mesh router via an 802.11 a/g link with a raw rate up to 54 Mb/s. It may take the client just a couple of seconds to download several tens of MP3 music files. This makes it highly desirable to minimize the authentication delay. Third, under conventional solutions, mesh routers will become very attractive targets and network entry points for DoS or distributed DoS (DDoS) attacks. For example, an attacker continuously sends fake authentication requests to a mesh router which, in turn, has to contact the home domains of the impersonated or even nonexistent users. If lots of collusive attackers launch this type of attack simultaneously, the resulting authentication signaling traffic will severely interfere with normal network signaling and data traffic. 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. Early adopters of wireless mesh technology include community net works, which can provide low-cost Internet access to whole neighbourhoods 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 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. The players in ARSA are brokers, users, and WMN operators whose relationship is analogous to that among a bank, a credit-card user, and a merchant. Each user acquires a universal pass from a broker whereby to enjoy ubiquitous WMN access. Once authenticating a pass, a WMN operator can grant access to the pass holder without fear of not being paid later. As compared with conventional home/foreign-domain solutions, ARSA does not require WMN operators to establish pair wise bilateral SLAs. Rather, each WMN operator merely needs to have an agreement with one or a few brokers whose number is considered much smaller than that of global WMN operators. In addition, mutual authentication and key agreement (AKA) between a mesh client and the serving WMN domain just involve local interactions without the real-time involvement of the corresponding broker. This is particularly beneficial for reducing authentication signaling overhead and latency. Furthermore, ARSA supports efficient pairwise AKA among mesh clients present in the same WMN domain. ARSA is also designed to be resilient to various attacks, including the location privacy attack, the denial-of-access attack, the bogus-beacon flooding attack, and the bandwidth-exhaustion attack.

II. PRELIMINARIES

A Security Requirements of WMNs Throughout this paper, we refer to the combination of the multihop wireless backbone, the wired APs, and any other WMN operator equipments, as the infrastructure. We also use the term "mesh" to indicate a subnet comprising a mesh router and its covered mesh clients. From a high-level point of view, we identify the following security requirements of WMNs. • Infrastructure security: This means the security of signaling and data traffic transmitted over the infrastructure. • Network access security: This indicates the communication security between a mesh client and a mesh router. It may also involve the communication security among mesh clients served by the same mesh router, if the route between a client and a router is in multiple hops. • Application security: This refers to the security of mesh clients' concrete data applications. Among them, infrastructure security is relatively easy to achieve since the infrastructure is under the full control of a WMN operator and the network elements of the infrastructure are typically stationary. Application security can also be easily achieved via high-layer security mechanisms such as IPsec, TLS, or VPNs. By contrast, network access security is much more difficult to ensure than the other two. One major reason is that mesh routers are designed to accept open access requests by most likely unknown mesh clients. Other notable causes include open access to the wireless channels and the dynamic network topology caused by the mobility of mesh clients. For lack of space, we focus on investigating network access security in this work, and leave the exploration of the other issues as future work. With respect to network access security, we recognize the following specific requirements, which are, however, not necessarily a complete list.

- Router-client authentication: A mesh router should authenticate a requesting client to prevent unauthorized network access. The client should also authenticate the router to shun bogus mesh routers of attackers.
- Router-client key agreement: The mesh router and the client should establish a shared key to encrypt and authenticate radio messages transmitted between them.
- Client–client authentication: This is required when one client forwards another's traffic to and from the mesh router. In general, each client should only

help other legitimate ones to get proper remuneration later.

- Client–client key agreement: If needed, two mesh clients should establish a shared key whereby to encrypt and authenticate the traffic between them.
- Location privacy: No entity other than a mesh client himself and a responsible location management authority (if any) should know both the real identity and the current location of the mesh client.
- Signaling authentication: The signaling data broadcast by a mesh router should always be authenticated to be distinguishable from those announced by an attacker.
- Service availability: A mesh router must be protected from DoS attacks and offer always available services.
- Incontestable billing: A mesh client should just pay what he ought to pay, while a WMN operator, as well as those clients forwarding traffic for others, receives the amount commensurate with the offered service.
- Secure routing: The routing protocol used inside a mesh should be secured against attacks.
- Secure MAC: The MAC protocol employed within a mesh must be resilient to attacks.

III. SYSTEM MODELS AND NOTATION

In this section, we present the network, trust, and pass models adopted in our ARSA, as well as the notation used. A. Network Model Future large-scale WMNs are expected to consist of a large number of WMN domains of different scales. Each WMN domain is operated by an independent operator and composed of a certain number of meshes, either physically adjacent or nonadjacent. For example, a WMN operator may own meshes in multiple cities or only in one city section. WMN domains may overlap with each other, and whether or not neighbouring domains are connected solely depends on operator policies. In general, a mesh router has much more powerful computation and communication capacities and abundant other resources than regular mesh clients. It is, therefore, reasonable to assume that a mesh router sends packets in one hop to all mesh clients in its coverage. By contrast, a mesh client may transmit packets in one hop or multiple hops to a mesh router within or beyond his transmission range. As noted in [1], a single-hop downlink can be highly beneficial. First, mesh clients can save their scarce energy, as there is no need to relay downlink packets. Second, a single-hop downlink can greatly facilitate the transmissions of control signaling packets from the mesh router to all mesh clients. Last, it renders the radio resource allocation performed by the mesh router much easier to implement. Note that, however, our ARSA can be easily extended for use in symmetric WMNs with both multihop uplinks and downlinks. It is worth pointing out that communications to and from a mesh router will be the major traffic pattern within a mesh. This is in line with the target use of WMNs, namely, relaying end users' traffic to and from the wired Internet. Such a unique traffic pattern would significantly reduce the routing complexity from mesh clients' point of view. The reason is that they only need to maintain a route to the mesh router instead of one route to each other client in the same mesh. To make ARSA independent of the underlying network implementations, we do not specify the MAC and routing protocols in use. Interested readers are referred to [2] for a detailed survey of candidate schemes.

A. Trust Model

The trust model of our ARSA is composed of a number of trust domains, each managed by a broker or WMN operator. To enjoy ubiquitous WMN access, each mesh client has to first register with at least one broker which, in turn, issues an electronic universal pass to the client. If enrolling in more than one broker, a client may accordingly own multiple passes. Each WMN operator is also required to have a trust relationship with one or a few brokers. It will grant network access to mesh clients holding valid passes issued by its trustable broker(s). In fact, one may view brokers as regular banks with which both mesh clients and WMN operators have opened accounts. We assume that brokers are fully trustable by both clients and operators, but a client and an operator usually do not play full trust on each other. The above trust model fits in well with ubiquitous Internet access via WMNs. Mesh clients see the advantage of being able to get on-demand network access by any WMN operator. The operators are relived from the heavy burden of establishing pair wise bilateral SLAs with potentially many other operators. Instead, each of them just needs to have a trust relationship with certain broker(s) whose number is considered much smaller than that of WMN operators. Furthermore, the operators have all mesh clients as potential customers, which is in contrast to the home/foreign-domain model, where a user is locked to a specific operator once signing an agreement. The brokers can make profits by deducing fees from an operator's credit or adding fees to a client's charge. They may also impose entry or subscription fees to mesh clients and operators for participation in their trust systems.

B. 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 manets 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 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 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 specification6 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.

Hybrid WMNs.

Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks, the routing capabilities of clients provide improved connectivity and coverage inside WMNs. The characteristics of WMNs are outlined below, where the hybrid architecture is considered for WMNs, since it comprises all the advantages of WMNs:

- WMNs support ad hoc networking, and have the capability of self-forming, self-healing, and self-organization.
- WMNs are multi-hop wireless networks, but with a wireless infrastructure/backbone provided by mesh routers.
- Mesh routers have minimal mobility and perform dedicated routing and configuration, which significantly decreases the load of mesh clients and other end nodes.
- Mobility of end nodes is supported easily through the wireless infrastructure.
- Mesh routers integrate heterogeneous networks, including both wired and wireless. Thus, multiple types of network access exist in WMNs.
- Power-consumption constraints are different for mesh routers and mesh clients.
- WMNs are not stand-alone and need to be compatible and interoperable with other wireless networks

Layered Communication Protocols Physical Layer Advanced Physical-Layer Techniques. Some advanced physical-layer techniques have been available for WMNs. Wireless radios of existing WMNs are able to support multiple transmission rates by a combination of different modulation and coding rates. With such modes, adaptive error resilience can be provided through link adaptation. Schemes such as orthogonal frequency multiple access (OFDM) and ultra-wide band (UWB) techniques are being used to support high-speed transmissions. In order to further increase capacity and mitigate the impairment by fading, delay-spread, and co-channel interference, multi-antenna systems such as antenna diversity, smart antenna, and MIMO systems, have been proposed for wireless communications. Although these physical-layer techniques are also desired by other wireless networks, it is a more challenging problem to develop such techniques for WMNs. For example, mesh networking among multiple nodes makes the system model much more complicated than that of a conventional MIMO system in wireless LANs or cellular networks.

In order to achieve much better spectrum utilization and viable frequency planning for WMNs, frequency-agile or cognitive radios are being developed to dynamically capture the unoccupied spectrum. The FCC has recognized the promising technique and is pushing to enable it to a full realization. Implementing cognitive radios on a software radio platform is one of the most powerful solutions, because all components of a radio, such as RF bands, channel access modes, and channel modulations, are programmable. The software radio platform is not a mature technology yet, although physical test beds are currently available. However, in the long run it will be a key technology for wireless communications because it can enable the programmability of all advanced physical layer techniques.

MAC Layer There exist differences between the MAC in WMNs and the classical counterparts for wireless networks:

- MAC for WMNs is concerned with more than one-hop communication.
- MAC is distributed, needs to be collaborative, and works for multipoint-to-multipoint communication.
- Network self-organization is needed for better collaboration between neighbouring nodes and nodes in multi-hop distances.
- Mobility is low but still affects the performance of MAC.

A MAC protocol for WMNs can be designed to work on a single channel or multiple channels simultaneously. Single-

Channel MAC. Three approaches are usually employed to design a single-channel MAC protocol for WMNs. Modifying Existing MAC Protocols. For example, in an IEEE 802.11 mesh network, the MAC protocol can be improved by adjusting parameters of CSMA/CA, e.g., contention window size, and modify back off procedures. However, such a solution can only achieve a low end-to-end throughput, because it cannot significantly reduce the probability of contentions among neighbouring nodes Multi-Channel MAC. To further improve network performance and also increase network capacity for WMNs, a favourable solution is to enable a network node to work on multiple channels instead of only on a single fixed channel. Depending on hardware platforms, different multi-channel MAC protocols need to be developed. Multi-Channel Single-Transceiver MAC. If cost and compatibility are the concern, one transceiver on a radio is a preferred hardware platform. Since only one transceiver is available, only one channel is active at a time in each network node. However, different nodes may operate on different channels simultaneously. To coordinate transmissions between network nodes under this situation, protocols such as the multi-channel MAC in [4] are needed. Multi-Channel Multi-Transceiver MAC. In this scenario, a radio includes multiple parallel RF front-end chips and baseband processing modules to support several simultaneous channels. On top of the physical layer, only one MAC layer module is needed to coordinate the functions of multiple channels. To the best of our knowledge, so far no multi-channel multi-transceiver MAC protocol has been proposed for WMNs.

Routing Layer Despite the availability of many routing protocols for ad hoc networks, the design of routing protocols for WMNs is still an active research area. We believe that an optimal routing protocol for WMNs must capture the following features:

- Multiple Performance Metrics. Many existing routing protocols use minimum hop-count as a performance metric to select the routing path. This has been demonstrated to be ineffective in many situations.
- Scalability. Setting up or maintaining a routing path in a very large wireless network may take a long time. Thus, it is critical to have a scalable routing protocol in WMNs.
- Robustness. To avoid service disruption, WMNs must be robust to link failures or congestion. Routing protocols also need to perform load balancing.
- Efficient Routing with Mesh Infrastructure.

Multi-Path Routing. The main objectives of using multi-path routing are to perform better load balancing and to provide high fault tolerance. Multiple paths are selected between source and destination. When a link is broken on a path due to a bad channel quality or mobility, another path in the set of existing paths can be chosen. Thus, without waiting to set up a new routing path, the end-to-end delay, throughput, and fault tolerance can be improved. However, given a performance metric, the improvement depends on the availability of node disjoint routes between source and destination. Another drawback of multi-path routing is its complexity. Hierarchical Routing. In hierarchical routing [1], a certain self-organization scheme is employed to group network nodes into clusters. Each cluster has one or more cluster heads. Nodes in a cluster can be one or more hops away from the cluster head. Since connectivity between clusters is needed, some nodes can communicate with more than one cluster and work as a gateway. When the node density is high, hierarchical routing protocols tend to achieve much better performance because of less overhead, shorter average routing path, and quicker set-up procedure of routing path. However, the complexity of maintaining the hierarchy may compromise the performance of the routing protocol. Moreover, in WMNs, a mesh client must avoid being a cluster head because it can become a bottleneck due to its limited capability. Geographic Routing. Compared to topology-based routing schemes, geographic routing schemes forward packets by only using the position information of nodes in the vicinity and the destination node [1]. Thus, topology change has less impact on the geographic routing than the other routing protocols. Early geographic routing algorithms are a type of single-path greedy routing schemes in which the packet forwarding decision is made based on the location information of the current forwarding node, its neighbors, and the destination node. However, all greedy routing algorithms have a common problem, i.e., delivery is not guaranteed even if a path exists between source and destination. In order to guarantee delivery, planar-graph-based geographic routing algorithms [1] have been proposed recently. However, these algorithms usually have much higher communication overhead than the single-path greedy routing algorithms.

Application Layer Numerous applications supported by WMNs can be categorized into several classes. Internet Access. Various Internet applications provide important timely information to people, make life more convenient, and increase work efficiency and productivity. In a home or small to medium business environment, the most popular network access solution is still DSL or cable modem along with IEEE 802.11 access points. However, compared with this approach, WMNs have many potential advantages: lower cost, higher speed, and easier installation. Distributed Information Storage and Sharing. Backhaul access to the Internet is not necessary in this type of applications, and users only communicate within WMNs. A user may want to store high-volume data in disks owned by other users, download files from other users’ disks based on peer-to-peer networking mechanisms, and query/retrieve information located in distributed database servers. Users within WMNs may also want to chat, talk on video phones, and play games with each other. Information Exchange across Multiple Wireless Networks. For example, a cellular phone may want to talk to a Wi-Fi phone through WMNs, or a user on a Wi-Fi network may expect to monitor the status in various sensors in a wireless sensor networks. Consequently, there are mainly three research directions in the application layer. Improve Existing Application Layer Protocols. In a wireless network, protocols in the lower layers cannot provide perfect support for the application layer. For example, as perceived by the application layer, packet loss may not always be zero, packet delay may be variable with a large jitter, etc. These problems become more severe in WMNs due to their ad hoc and multi-hop communications. Such problems can fail many Internet applications that work smoothly in a wired network. Propose New Application-Layer Protocols for Distributed Information Sharing. Currently, many peer-to-peer protocols are available for information sharing on the Internet. However, these protocols cannot achieve satisfactory performance in WMNs since WMNs have much different characteristics than the Internet. Develop Innovative Applications for WMNs. Such applications must bring tremendous benefits to users, and also cannot achieve best performance without WMNs. Such applications will enable WMNs to be a unique networking solution instead of just another option for wireless networking.

IV.CONCLUSION

Although WMNs can be built up based on existing technologies, field trials and experiments with existing WMNs prove that the performance of WMNs is still far below expectations. As explained throughout this article, there still remain many research problems. Among them, the most important and urgent ones are the scalability and the security.

Scalability. Based on existing MAC, routing, and transport protocols, network performance is not scalable with either the number of nodes or the number of hops in the network. This problem can be alleviated by increasing the network capacity through using multiple channels/radios per node or developing wireless radios with higher transmission speed. However, these approaches do not truly enhance the scalability of WMNs, because resource utilization is not actually improved. Therefore, in order to achieve scalability, it is essential to develop new MAC, routing, and transport protocols for WMNs.

Security. WMNs are vulnerable to security attacks in various protocol layers. Current security approaches may be effective to a particular attack in a specific protocol layer. However, there still exists a need for a comprehensive mechanism to prevent or counter attacks in all protocol layers. Moreover, self-organization and self-configuration capability is a desired feature in WMNs. It requires protocols in WMNs to be distributive and collaborative. However, current WMNs can only partially realize this objective. Furthermore, current WMNs still have very limited capabilities of integrating heterogeneous wireless networks, due to the difficulty in building multiple wireless interfaces and the corresponding gateway/bridge functions in the same mesh router.

REFERENCES

[1] R. Roy, Handbook of Mobility Models and Mobile Ad Hoc Networks. Springer, 2010.

[2] Y.-C. Chen, E. Rosensweig, J. Kurose, and D. Towsley, “Group Detection in Mobility Traces,” Proc. Sixth Int’l Wireless Comm. and Mobile Computing Conf. (IWCMC ’10), 2010.

[3] T. Camp, J. Boleng, and V. Davies, “A Survey of Mobility Models for Ad Hoc Network Research,” Wireless Comm. and Mobile Computing, vol. 2, no. 5, pp. 483-502, 2002.

[4] X. Hong, M. Gerla, G. Pei, and C. Chiang, “A Group Mobility Model for Ad Hoc Wireless Networks,” Proc. Second ACM Int’l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM ’99), 1999.

[5] K. Blakely and B. Lowekamp, “A Structured Group Mobility Model for the Simulation of Mobile Ad Hoc Networks,” Proc. Second Int’l Workshop Mobility Management & Wireless Access Protocols (MobiWac), 2004.

[6] Y. Zhang and Y. Fang, “ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks,” IEEE J. Selected Areas in Comm., vol. 24, no. 10, pp. 1916-1928, Oct. 2006.

[7] J. Sun, C. Zhang, and Y. Fang, “A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks,” Proc. IEEE INFOCOM, 2008.

[8] B. Salem and J. Hubaux, “Securing Wireless Mesh Networks,” IEEE Wireless Comm., vol. 13, no. 2, pp. 50-55, Apr. 2006.

[9] T. Shuai and X. Hu, “Connected Set Cover Problem and Its Applications,” Proc. Second Int’l Conf. Algorithmic Aspects in Information and Management, pp. 243-254, 2006.