Ann. Telecommun. (2009) 64:401–413
DOI 10.1007/s12243-008-0084-8

A robust security scheme for wireless mesh enterprise networks

Md. Abdul Hamid · M. Abdullah-Al-Wadud · Choong Seon Hong · Oksam Chae · Sungwon Lee

Received: 5 August 2008 / Accepted: 23 December 2008 / Published online: 23 January 2009

Abstract In this paper, we address the security challenges for wireless mesh enterprise networks (WMENs). The topology and communication characteristics of WMEN include the following: (a) deployment of the network devices are not planar, rather, devices are deployed over three-dimensional space (e.g., office buildings, shopping malls, grocery stores, etc.); (b) messages, generated/received by a mesh client, traverse through mesh routers in a multihop fashion; and (c) mesh clients, being mostly mobile in nature, may result in misbehaving or be spurious during communications. We propose a security scheme for WMEN in order to ensure that only authorized users are granted network access. Particularly, our scheme includes: (a) a deterministic key distribution technique that perfectly suits the network topology, (b) an efficient session key establishment protocol to achieve the client–router and router–router communications security, and (c) a distributed detection mechanism to identify malicious clients in the network. Analytical and simulation results are presented to verify our proposed solutions.

Keywords Wireless mesh enterprise networks · Key distribution · Communications security · Malicious client detection

1 Introduction

The continuing driving force in the development of wireless mesh networks (WMNs) comes from their envisioned advantages, including extended coverage, robustness, self-configuration, easy maintenance, and low cost. These aspects attract the interests towards a wide variety of potential applications and usage scenarios for the mesh networking domain. WMN is an emerging two-tier architecture based on wireless multihop transmission. A WMN is composed of wireless mesh clients (MCs) and wireless mesh routers (MRs). The latter offers connectivity to the former by acting like access points, forming, at the same time, a self-organized wireless backbone. This backbone has two possible roles. It can be either a stand-alone network simply offering interclient connectivity or it can be a local extension for the wired Internet if there are available connections between one or more gateways. In both cases, the WMN's backbone is in charge of relaying all the traffic from/to MCs. A comprehensive survey on WMNs and related issues is given in [1], while an architecture example of WMNs is given in [2].

Mesh networks have the potential to bring diverse advantages to wireless communications services, allowing clients to exchange information in a decentralized

Md. A. Hamid · M. Abdullah-Al-Wadud ·
C. S. Hong (✉) · O. Chae · S. Lee
Department of Computer Engineering,
School of Electronics and Information,
Kyung Hee University, 1 Seocheon, Giheung, Yongin,
Gyeonggi 446-701, South Korea
e-mail: cshong@khu.ac.kr

Md. A. Hamid
e-mail: hamid@networking.khu.ac.kr

M. Abdullah-Al-Wadud
e-mail: awsujon@yahoo.com

O. Chae
e-mail: oschae@khu.ac.kr

S. Lee
e-mail: drsungwon@khu.ac.kr

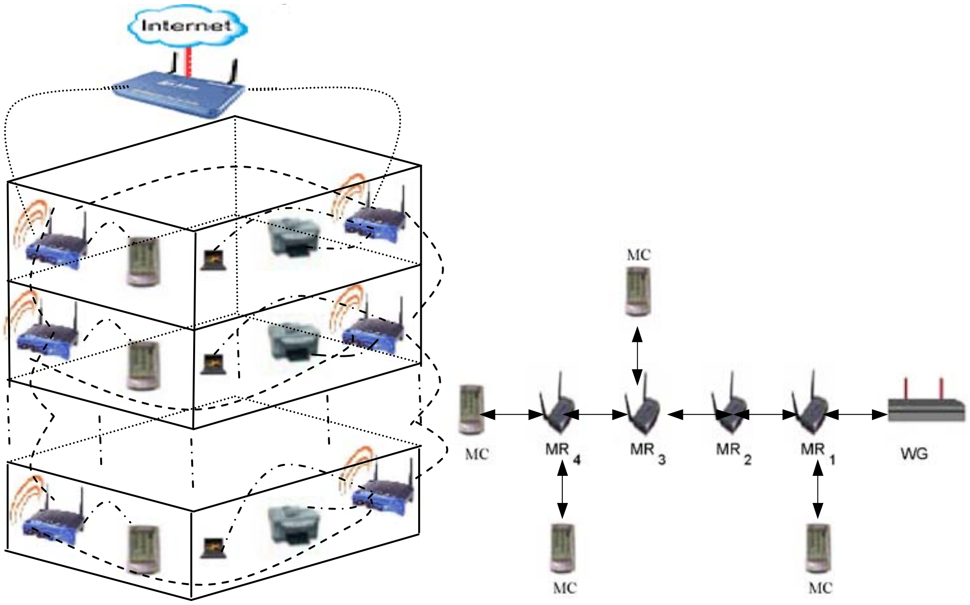
manner and also to extend coverage of cellular and other networks by allowing relay-based networking at the edge terminals. Most of the technical challenges in mesh networks depend to a large extent on the environments and usage scenarios in which WMNs are used [1]. One form of WMN, called wireless mesh enterprise network (WMEN), may be defined as a small network within an office or a medium-sized network for all offices in an entire building, or a large-scale network among offices in multiple buildings [1]. Though standard IEEE 802.11 is being widely used in various offices, enterprise networks are costly since connections among these networks need to be achieved through wired Ethernet connections. If the access points are replaced by MRs, as shown in Fig. 1a, Ethernet wires can be eliminated. WMNs can grow easily as the size of the enterprise expands. The service model of enterprise networking can be applied to many other public and commercial service networking scenarios such as airports, hotels, shopping malls, convention centers, sport centers, etc. [1]. Since mesh enterprise network is a viable and cost-effective solution for building automation, security is turning out to be a very high concern. Particularly, communication security mechanisms and intrusion detection systems become a necessity for enterprise buildings, shopping malls, grocery stores, etc. [1]. However, security issues in the domain of mesh networks are still in their infancy, as very little attention has been devoted to this very topic (especially in WMEN) by the research community. Before identifying the security problems, let us categorize the communication scenarios in a typical mesh enterprise network as depicted in Fig. 1b.

(a) *Client–router communications*: Usually, MCs are associated with a router in one-hop to send/receive data packets and routers are responsible to relay/forward packets to/from clients.

(b) *Router–router communications*: A set of stationary MRs form the wireless backbone of a WMEN and data must traverse using these backbone routers possibly in a multihop fashion.

(c) *Router–gateway communications*: As MRs are connected to the wired infrastructure/Internet via wireless gateway(s) (WG), they must rely on the WG to relay their data to/from the Internet.

To identify the security problems, let us carefully analyze the underlying characteristics of the topology and communication scenarios of a mesh enterprise network based on Fig. 1. Figure 1a shows a possible topology of WMEN where the network is deployed in an office building. If nodes of a network are distributed over a three-dimensional (3D) space (e.g., in a multi-floored building), it essentially differs from the design of two-dimensional (2D) terrestrial networks where it is assumed that all nodes reside on a plane [3]. Most often, 2D schemes are applied in 3D scenarios, ignoring the third dimension. To some extent, this approach is justified and applicable without experiencing major drawbacks. However, in some cases, 2D projections may not provide a clear view of actual 3D scenarios. For



(a) (b)

Fig. 1 WMN for enterprise networking. **a** A mesh enterprise network deployed in a multifloored building. **b** A typical communication scenario: Mesh routers (*MRs*) offer connectivity to mesh clients (*MCs*) by acting like access points and wireless gateways (*WG*). MRs are also in charge of relaying all traffic from/to MCs in a multihop fashion

example, a 3D network topology may have a negative impact on 2D geographical routing protocols (but not on other routing protocols or security schemes). In many tall buildings, two nodes may be found at exactly the same (x, y) location but on different floors; any 2D model would assume that they are in the same location, and yet, they are not. Therefore, a modest contribution towards ameliorating a key distribution and communication security problem is crucial to suit 3D characteristics of the network topology.

Figure 1b depicts the communications scenario where MRs provide connectivity and relay packets from/to MCs in a multihop fashion. Mutual authentication between client–router and router–router is a prerequisite for secure exchange of messages (generated or received by a client). The use of public key cryptography to authenticate the sender and receiver for every packet results in additional delays due to high computational complexity. Moreover, using public key for authentication requires signature generation and verification, which may lead to high computational overhead and denial-of-service (DoS) attack, respectively [4]. So, it is preferable to develop an authentication scheme based on symmetric key cryptography for the communication scenarios described herein.

For WMEN, it is reasonable to assume that all the MRs are static and MCs are mobile (since the network is deployed in a building, e.g., office buildings, shopping malls, etc.). So, the WMEN is compounded by the fact that MCs are dynamic in the sense that they are free to join and leave at will. Since the clients communicate with their associated routers using the carrier sense multiple access/collision avoidance (CSMA/CA) based protocol (in IEEE 802.11 DCF mode [5]) to access the medium, some clients may maliciously exploit the access mechanism to get a higher share of bandwidth. CSMA/CA protocols rely on the random deferment of packet transmissions. Like most other protocols, CSMA/CA was designed with the assumption that the devices (users) would play by the rules. This can be dangerous, since the devices themselves control their random deferment. Indeed, with the higher programmability of the network adapters, the temptation to tamper with the software or firmware is likely to grow. Therefore, in the presence of malicious clients (even though they are legitimate in the sense that they use cryptographic keys and obey the underlying security protocol) that disobey the standard, the bandwidth share of the well-behaved clients may significantly degrade [6, 7]. Since all the wireless stations use the similar IEEE 802.11 CSMA/CA medium access control protocol, malicious use of the medium is always possible to gain higher share of bandwidth at the expense of other users in the network. Even though the cryptographic solution may achieve authentication, data confidentiality, and other security issues, this mechanism may not detect/restrict the medium access control layer greedy behavior since wireless devices (e.g., MCs) directly deal with the wireless medium [6]. For network survivability and reliability, it is necessary to develop an efficient technique to detect misbehaving client(s) to defend the network being crippled. Therefore, along with the cryptographic solution, a detection mechanism, as a second line of defense, is presented to defend/restrict malicious clients.

In this paper, we focus on devising the security solutions for client–router and router–router communications, and we do not consider router–gateway communication security problems as strong security may be achieved with a powerful gateway. We design the security solutions for WMEN based on our previous work presented in [8]. The main contribution of this paper is to be of three-fold significance:

(a) We use the 3D geometry to design an efficient deterministic key distribution technique that suits the underlying network topology of WMEN depicted in Fig. 1a. We analyze the security strength to show that the distribution technique is robust against small-scale attacks (i.e., when the number of nodes compromised is small) compared to well-known deterministic key distribution schemes.

(b) We propose a session key establishment (SKE) protocol to achieve communications security between client–router and router–router using the proposed key distribution technique. We show that SKE protocols require less computation and communication overheads.

(c) Finally, we present a distributed detection mechanism to identify unpredictable presence of a misbehaving/malicious client in the network. Through simulation, we evaluate the proposed mechanism and results show that it yields high detection and low false positive rates.

Throughout this paper, we use the notations shown in Table 1. The rest of the paper is organized as follows. Section 2 describes related works and Section 3

Table 1 Notations used throughout this paper

Notation	Meaning
MR	Mesh router
MC	Mesh client
WG	Wireless gateway
nonce	Time stamp
$\|\|$	Concatenation
$K_{(A,B)}$	Shared session key between devices A and B
$E(K, \text{msg})$	Encryption of message msg with key K
$\text{MAC}(K, \text{msg})$	Message authentication code using msg and K

describes the system model and assumptions. We present our security scheme in detail in Section 4. Malicious client detection mechanism is presented in Section 5. Finally, Section 6 concludes our work.

2 Related works

2.1 Security in WMNs

In the state-of-the-art research, security issues in WMNs have been given a little attention in the research community. In [4], the authors have identified that the network operations that need to be secured in WMN are detecting corrupted routers, securing routing protocols, and enforcing a fairness metric. They also referred to adapting existing solutions proposed for ad hoc network security. However, they ignored the class of attacks and malicious behavior of MCs. Zhang et al. in [9] have come up with an attack-resilient security architecture for multihop WMNs. They have modeled WMN architecture as a credit card-based e-commerce system and showed that an MC does not need to be bound to a specific WMN operator; rather, this client gets ubiquitous network access by a universal pass issued by a third-party broker. They used an identity-based public key cryptosystem for authentication and key agreement between MCs and routers. References [10] and [11] have addressed the issue of privacy in WMN. However, both focused on the traffic privacy by proposing some anonymous routing algorithm. They have ignored how to deal with identity privacy and not mentioned how authentication and key agreement are performed between mesh nodes. As of now, only [12] have shown an effective way to model a node-capture attack in multihop WMN by formulating it as an integer-linear programming minimization problem. They claimed that privacy-preserving key establishment protocols can help to prevent minimum cost node capture attack.

In [13], the authors have proposed an active cache-based mechanism to defend DoS attack caused by flooding a large volume of traffic in the network by malicious intruders. They have exploited the most frequently used caching mechanism to identity flooding and raise an early alert to defend the attack. Based on the detection method of medium access control layer selfish behavior in wireless ad hoc networks developed in [6], authors presented a selfish behavior detection model in [14] with a double-mode detection mechanism in WMN. Different detection mechanisms are used for router and client selfish attacks. A malicious client detection algorithm is developed in [8] based on the existing communication history for two communicating MCs with a common set of routers (CSRs) in WMEN. Common set is chosen based on the close relationship with the two communicating clients. For example, all the past messages between clients p and q traverse through this set of routers and/or both clients have individual communications with those routers, and therefore, they have an existing trust history with the routers. Based on this trust relationship, an algorithm is developed to calculate the correlation between clients p and q, and a decision as to whether client q is malicious or not is sent to client p at the time client p wants to communicate with q. The algorithm works well when a client behaves maliciously (i.e., obtaining a higher share of bandwidth) with all the routers. However, if the client strategically behaves maliciously with selective routers, then it might maintain the average correlation (with CSRs) higher than a detectable threshold value. Furthermore, to detect whether client q is malicious or not, an MR has to request each of the common routers between clients p and q about their ratings (i.e., trust values), and this introduces delay and communication overhead. In [15], the authors identified attacks (such as coordinate deflation, oscillation, disruption, and pollution attacks) targeting the underlying virtual coordinate system for wireless sensor networks. Authors exploit the Wilcoxon signed rank test (WSRT) technique [16] to design a detection mechanism to mitigate coordinate deflation attacks that cause a decrease of hop count for a large portion of nodes in the network. The novel use of the Wilcoxon test-based detection mechanism in [15] and the accuracy (and simplicity) of the Wilcoxon test itself motivate us to use it (i.e., Wilcoxon test) to enhance our previous work [8] for accurate detection of the malicious client(s).

2.2 3D wireless networks

In the literature, a lot of effort has been dedicated to develop a protocol for wireless networks considering 3D geometry. However, existing protocols focus on placement of the nodes, routing strategy, or capacity in 3D wireless networks. Security considerations in 3D networks, especially in the domain of WMN, remain unfocused. In the following, we review the existing works in the field of 3D wireless networks.

A detailed explanation on different kinds of polyhedrons and other necessary background information on 3D networks are provided in [3]. Assuming that nodes can be placed at any arbitrary location, authors in [3] developed a placement strategy of the nodes in 3D such that the number of nodes required for surveillance of a 3D space is minimized. They also provide the minimum ratio of the transmission range and sensing range required for such a placement strategy. Extremal properties have been achieved in [17] with various critical transmitting/sensing ranges for connectivity and coverage in 3D wireless sensor networks. A fault-tolerant topology control algorithm is presented in [18] for multihop wireless networks by varying the transmission power at each node. Each node decides its power based on local information about the relative angle of its neighbors and forms a fault-tolerant connected network. Capacity of 3D wireless networks is obtained in [19] and authors have shown that they have higher capacity than 2D networks. Authors conclude that a wireless network connecting fewer number of users, or allowing connections mostly with nearby neighbors, may be more likely to find acceptance in terms of throughput that can be achieved. A logical coordinate-based routing is presented in [20], and it is shown to be efficient in that it needs only one-hop neighborhood information and not two. Akyildiz et al. [21] investigated fundamental key aspects of underwater acoustic communications in which different architectures for 2D and 3D underwater sensor networks are discussed, and the characteristics of the underwater channel are detailed. References [22] and [23] studied 3D cellular networks, each cell is represented as rhombic dodecahedron in [22], and hexagonal prism-shaped cells are used in [23]. Both works have focused to extend the standard concept of planar cellular networks into space.

3 System model and assumptions

We consider an IEEE 802.11s [24] based WMEN. There are N MRs denoted as MR_j, where $j = 1, 2, \ldots, N$, and a WG that form the infrastructure mesh. All the MRs are connected to the gateway WG in multihop fashion and the WG connects the network to an external network (i.e., Internet). Each MR_j can act as an access point and a relay node. There are n_j MCs (users) denoted as $\mathrm{MC}_{j,i}$, where $i = 1, 2, \ldots, n_j$, attached to (associated with) MR_j in one hop using the existing wireless LAN technologies; for example, 802.11 (WiFi). For simplicity, we use MC_i to denote MC $\mathrm{MC}_{j,i}$ throughout this paper. In general, an MR has much more powerful computation and communication capacities and other abundant resources than regular MCs. An example of IEEE 802.11s-based WMN is shown in Fig. 1a for enterprise networking [1].

We assume that there exists an operator who is responsible for the deployment and overall management of the WMEN including key management issues such as the generation, distribution, and refreshment of the keys. We consider that MRs are under the full control of the operator and are trusted by that operator. We assume that only MCs misbehave to obtain a higher share of bandwidth.

4 Security scheme

In this section, we present the proposed security scheme for WMEN in detail. First, we provide the insight of the basic 2D matrix-key distribution technique [25] in Section 4.1. Then, a 3D matrix key distribution technique is engineered in Section 4.2 to apply to mesh enterprise networks. In Section 4.3, we develop a SKE protocol for router–router and client–router communications. Finally, we analyze the proposed security scheme in Section 4.4. We describe each of the components in the sequel.

4.1 Basic matrix key distribution

Suppose that there are N nodes in an $m \times m$ space, where $N = m^2$, and each node is assigned a position (i, j) and is denoted as n_{ij}. Similarly, there are N keys, denoted as k_{ij}. A key server generates the keys at random and gives node n_{ij} a set of keys which consists of all the keys that are on either the same row or column as n_{ij}. Hence, n_{ij} gets the keys according to Eq. 1

$$K_{ij} = \{k_{xy} | x = i \text{ or } y = j\}. \tag{1}$$

When node A (n_{ij}) wants to communicate with B (n_{uv}), it simply finds out B's position (u, v) and uses the keys k_{iv} and k_{uj} that are common between A and B to compose a session key (Fig. 2).

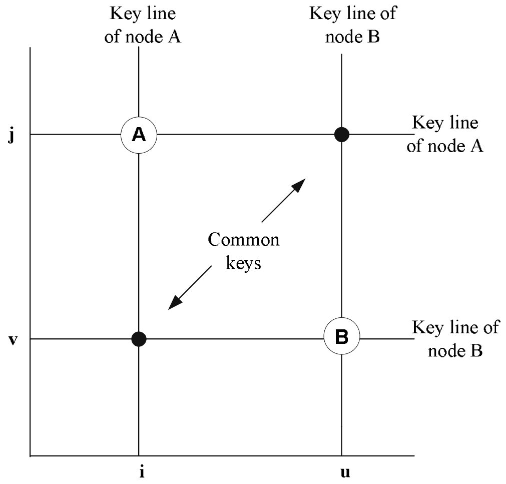


Fig. 2 Conventional matrix-key distribution

The weakness of this protocol is that, if node A and B are on the same line or column, any node on the same line or column may compromise the session because it shares the same common keys used between A and B. When A and B are not on the same line or column, the situation is better as two correctly positioned colluding nodes are needed to compromise the session key. To overcome this drawback, a multiline protocol is developed in [25] by allocating more key lines to each node instead of only two, as in the basic scheme. In multiline protocol, the key set of node n_{ij} is assigned according to Eq. 2

$$K_{ij} = \{k_{xy} | y - j + C_l(x - i) = 0 \bmod(m)\}, \tag{2}$$

where, $l = 1, 2, \ldots, t$ and $C_p \neq C_q$ when $p \neq q$.

Here, the key set is a set of t lines on the $m \times m$ matrix all passing through point (i, j). If two nodes n_{ij} and n_{uv} want to find a common key, they solve $t(t-1)$ linear equation groups, each of which has the form of Eq. 3

$$\left.\begin{aligned} y - j + C_p(x - i) = 0 \bmod(m) \\ y - v + C_q(x - u) = 0 \bmod(m) \end{aligned}\right\}, \tag{3}$$

where, $p, q = 1, 2, \ldots, t$ and $p \neq q$.

The solutions (x, y) are positions on the matrix of keys that nodes n_{ij} and n_{uv} have in common. Interested readers may further refer to [25] for clear understanding of the basic matrix key scheme.

4.2 Key distribution for WMEN

We make use of 3D geometry to design a deterministic key distribution technique for WMEN. In our scheme, the deployment space (as shown in Fig. 1a) is divided into N cells of an $m \times m \times m$ cubic matrix, where $N \leq m^3$ and $m > 2$. The space is the set m^3 of ordered triples (i, j, k), where i, j, k are real numbers. The triple (i, j, k) is called a point or location in m^3. Similarly, there are m^3 secret keys, one for each location (i, j, k), where $(i, j, k) = 0, 1, 2, \ldots, m-1$. Then, $N(N \leq m^3)$ MRs are placed one in each cell with location (i, j, k). Our key distribution technique ensures that each MR MR_{ijk} is assigned a key set K_{ijk} that includes a key corresponding to its location (i, j, k), as well as keys from other locations. So, K_{ijk} is the set of keys that a MR MR_{ijk} gets according to Eq. 4

$$\begin{aligned} K_{ijk} = \{k_{xyz} | z - k + C_p^{\alpha}(y - j) + C_p^{\beta}(x - i) \\ = 0 \bmod(m)\}. \end{aligned} \tag{4}$$

Equation 4 is a plane and, hence, contains m^2 locations. Thus, a router MR_{ijk} in location (i, j, k) gets m^2 keys from the m^3 locations satisfying Eq. 4.

To find common keys between any two communicating routers, say, MR_{ijk} and MR_{uvw}, they need to solve the following system of linear equations given by Eq. 5

$$\left.\begin{aligned} z - k + C_p^{\alpha}(y - j) + C_p^{\beta}(x - i) = 0 \bmod(m) \\ z - w + C_q^{\alpha}(y - v) + C_q^{\beta}(x - u) = 0 \bmod(m) \end{aligned}\right\}, \tag{5}$$

where, $(C_p^{\alpha} - C_q^{\alpha}) \neq 0 \bmod(m)$ OR $(C_p^{\beta} - C_q^{\beta}) \neq 0 \bmod(m)$, when $p \neq q$ (i.e., plane p and plane q are not parallel). In fact, Eq. 5 specifies two communicating routers' key rings (i.e., key-chains) from two nonparallel planes p and q, and the common points (x, y, z) of two planes shape a line with m locations. So, the solutions (x, y, z) of Eq. 5 are the positions of m keys that nodes MR_{ijk} and MR_{uvw} have in common.

From the distribution technique, each router MR is preloaded with m^2 keys. Let us assume that there are n MCs under each MR. The WMEN operator may assign each MC a subset ζ keys from these m^2 keys according to Eq. 6

$$\zeta = Max\{\lfloor m^2/n \rfloor, 1\}. \tag{6}$$

We require $m^2 \geq n$ in Eq. 6 to ensure that each of the n MCs under a router has one or more distinct keys. However, if n is too large, then a higher value of m^2 is required to satisfy this inequality. We can achieve this by increasing the size of the matrix (i.e., increasing the number of locations (keys) in the same space). This will result in higher m^2, i.e., more keys in the key-chains of MRs. This will leave some locations in the matrix empty, where no MR is placed but keys are assigned to be used by MRs at other locations.

In our approach, in a WMEN with $N(N \leq m^3)$ MRs and n MCs under each MR, each MR has a key-chain of m^2 keys, and any two communicating MRs have m keys in common in their key-chains to secure router–router communications and each MC has ζ keys in common with its corresponding router to secure client–router communications. We illustrate our proposed distribution technique by the following example.

Example Let us consider a simple example with $N = 27$. According to the proposed technique, the distribution is (m^3, m^2, m). Twenty seven locations are ordered in $3 \times 3 \times 3$ space as $(0, 0, 0), (0, 0, 1), \ldots, (2, 2, 2)$ and 27 keys and routers are placed in 27 locations, with one key in each location with key identifiers $1, 2, \ldots, 27$. Let us randomly pick three MRs, MR_{201}, MR_{012}, and MR_{222}, from locations (2, 0, 1), (0, 1, 2), and (2, 2, 2) with constant set $(C_p^{\alpha}, C_p^{\beta})$, being (2, 6), (7, 3), and (4, 8), respectively. According to (4), these three routers get the key sets (2, 6, 7, 11, 15, 16, 20, 24, 25), (1, 6, 8, 10, 15, 17, 19, 24, 26), and (3, 5, 7, 10, 15, 17, 20, 22, 27). From the example, it is observed that each router has nine keys and between any two routers, there are three keys in common to secure their communications. Furthermore, three routers have exactly one key in common, i.e., two nonparallel planes have common locations that lie on an intersecting line and three nonparallel planes (i.e., any two of the three planes are not parallel) have exactly one location (key) in common. If there are three MCs attached to each router, then each MC gets $\zeta = 3$ keys to secure their communications with their corresponding MRs.

4.3 Session key establishment

A session key is an ephemeral secret, i.e., one whose use is restricted to a short time period such as a single session, after which all traces are eliminated. So, instead of using direct shared keys, two nodes may compute a session key from their shared keys to secure their communications. In this section, we present the SKE procedures for router–router and client–router communications, and we show how they may exchange messages securely.

Router–router SKE: From the key distribution technique described in Section 4.2, it can be seen that two communicating routers may easily find common keys without requiring any message exchange; rather, they need to compute a linear equation group (Eq. 5) provided that they know each other's location information. Here, we show that two communicating routers may establish a session key from m common keys using any predefined secure function without any message exchange. Two routers MR_u and MR_v may compute a session key using simple exclusive OR operations as Eq. 7

$$K_{(\mathrm{MR}_u,\mathrm{MR}_v)} = k_1 \oplus k_2 \oplus \cdots \oplus k_m. \quad (7)$$

Then, using this session key, both routers may exchange messages securely and verify message integrity. For example, router MR_u sends a message, msg, to MR_v according to Eq. 8

$$\mathrm{MR}_u \rightarrow \mathrm{MR}_v : \mathrm{MAC}(K_{(\mathrm{MR}_u,\mathrm{MR}_v)}, \mathrm{msg}),$$
$$E(K_{(\mathrm{MR}_u,\mathrm{MR}_v)}, \mathrm{msg}). \quad (8)$$

Client-router SKE: A MC $\mathrm{MC}_i(i \in n)$ may establish a pair-wise session key with its corresponding router, $\mathrm{MR}_j(j \in N)$ using one of its ζ keys prior to sending messages. To establish a session key, MC_i unicasts a key negotiation message to communicate with MR_j as Eq. 9

$$\mathrm{MC}_i \rightarrow \mathrm{MR}_j : \mathrm{ID}_{\mathrm{MC}_i}, \mathrm{ID}_{k_i}, \mathrm{nonce}_{\mathrm{MC}_i},$$
$$\mathrm{MAC}(k_i, \mathrm{ID}_{\mathrm{MC}_i}||\mathrm{ID}_{k_i}||\mathrm{nonce}_{\mathrm{MC}_i}). \quad (9)$$

MR_j authenticates MC_i by checking message authentication code (MAC) and accordingly unicasts a message to compose a session key with the shared key $k_i \in \zeta$ as Eq. 10

$$\mathrm{MR}_j \rightarrow \mathrm{MC}_i : \mathrm{ID}_{\mathrm{MR}_j}, \mathrm{nonce}_{\mathrm{MR}_j},$$
$$\mathrm{MAC}(k_i, \mathrm{ID}_{\mathrm{MR}_j}||\mathrm{nonce}_{\mathrm{MR}_j}). \quad (10)$$

Finally, each party (both MR_j and MC_i) derives the session key $K_{(\mathrm{MR}_j,\mathrm{MC}_i)}$ according to Eq. 11

$$K_{(\mathrm{MR}_j,\mathrm{MC}_i)} = \mathrm{MAC}(k_i, \mathrm{nonce}_{\mathrm{MR}_j}||\mathrm{nonce}_{\mathrm{MC}_i}). \quad (11)$$

Then, using this session key, both the router and the client may exchange messages securely and verify message integrity. For example, client MC_i sends a message msg to MR_j according to Eq. 12

$$\mathrm{MC}_i \rightarrow \mathrm{MR}_j : \mathrm{MAC}(K_{(\mathrm{MR}_j,\mathrm{MC}_i)}, \mathrm{msg}),$$
$$E(K_{(\mathrm{MR}_j,\mathrm{MC}_i)}, \mathrm{msg}). \quad (12)$$

Since clients are mobile, they may leave (disassociate) their corresponding MRs and join (reassociate) other MRs in the network. As client–router session key is derived using one of the shared keys between them (i.e., the client and the corresponding router), when a client moves and gets attached to a new MR, the client has to get a new key set ζ from the new MR and, accordingly, both MC and MR may derive session keys to achieve communication security in the similar manner described above. However, a client needs to associate with an MR before getting the keys form the corresponding MR. To associate with an MR, an MC needs to follow some specific association protocol (such as association request/reply of IEEE 802.1X access control mechanism [26]) to access the network. Similarly, when an MC moves from one MR to another MR, this MC reassociates itself with the new MR to access the network in a similar manner. After a successful (re)association, the MC gets a subset ζ keys from the corresponding MR.

Establishment of a session key (between an MC and an MR) requires two key negotiation messages, one unicast message transmitted by the MC to the MR (Eq. 9) and one unicast message transmitted by the MR to the MC (Eq. 10), using the shared key between them. To exchange these key negotiation messages, MC and MR may use any standard messaging protocol available at link or network layer. For instance, Internet Control Message Protocol [27] can be used to exchange key negotiation messages in client–router SKE phase.

4.4 Analysis

Security: The proposed deterministic key distribution design has the property that the probability of any pair of nodes sharing a key is 1, and so, the average key-path length is 1. Keeping this property, we are interested to compare the resilience of the key distribution technique with the deterministic scheme based on combinatorial design theory [28]. Particularly, we compute the probability that a specific random communication link between two random routers A and B is compromised when an adversary has captured x routers that do not include router A or B.

We assume that the attacker has the ability to monitor the whole network and selects the routers wisely. Since the key-chain size is m^2 and a key can appear in m^2 locations according to our distribution technique, an attacker needs at least m^2 key-chains to be able to recover the key pool. A wise attacker may selectively capture the nodes that have the same specific key in their key-chains, and there are m^2 such key-chains for our scheme. Therefore, in our scheme, probability p_c that a link is compromised when an attacker captures x key-chains (i.e., fraction of compromised links between uncompromised routers) can be given as Eq. 13

$$p_c = \left(1 - \frac{\binom{m^3-m^2}{x}}{\binom{m^3}{x}}\right). \tag{13}$$

As two communicating routers establish link keys (i.e., session key) with m common keys between them, the probability $p_c(m)$ that all the m keys are correctly compromised is given by Eq. 14

$$p_c(m) = \left(1 - \frac{\binom{m^3-m^2}{x}}{\binom{m^3}{x}}\right)^m. \tag{14}$$

In [28], a deterministic key distribution approach is presented using combinatorial design theory. Combinatorial design theory provides a method to arrange elements of a finite set into subsets to satisfy certain properties. A balanced incomplete block design (BIBD) is one of such designs. Authors use the finite projective plane (which is a subset of symmetric BIBD) to design their key distribution scheme. The finite projective plane consists of a finite set P of points and a set of subsets of P, called lines. For an integer q where q is prime and $q \geq 2$, the finite projective plane of order q has four properties: (a) every line contains exactly $(q+1)$ points, (b) every point occurs on exactly $(q+1)$ lines, (c) there are exactly (q^2+q+1) points, and (d) there are exactly (q^2+q+1) lines. If lines are considered as key chains and points as nodes, then a finite projective plane of order q is a design with parameters $(q^2+q+1, q+1, 1)$, where (q^2+q+1) is the total number of keys (nodes), $(q+1)$ is the key-chain size for each node, and there is only one common key between any two nodes. With this design, the probability p_c^{comb} that a link is compromised when an attacker compromises x key-chains (nodes) is given in [28] as Eq. 15

$$p_c^{\text{comb}} = \left(1 - \frac{\binom{q^2}{x}}{\binom{q^2+q+1}{x}}\right). \tag{15}$$

In Fig. 3, the security strength of the proposed scheme is compared with combinatorial design approach based on Eqs. 14 and 15, respectively. As depicted in Fig. 3, the security strength for the proposed scheme outperforms the combinatorial design of key distribution when the number of compromised nodes (number of routers in our case) is relatively small while both the schemes provide key share probability 1. Since there is only one common key between any two nodes in the combinatorial design approach, this key is used to secure the link between two communicating nodes. In our approach, instead of one, more keys are used to secure the link (since m keys are common between any two nodes), which increases the communication security between two neighboring nodes compared to the combinatorial design. In our scheme, since the key chain size is higher than that of the combinatorial design scheme, when the number of compromised nodes (i.e., routers) is high, our scheme sacrifices resilience

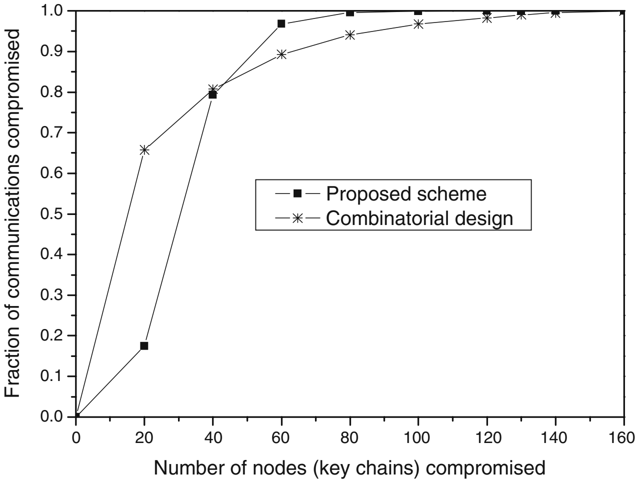


Fig. 3 Resilience comparison of the proposed key distribution scheme with the combinatorial design of key distribution mechanism in [28]. Results are compared for the same key pool size of 1,331 keys (nodes). Probability that a specific random communication link between two random nodes A and B is compromised when an adversary has captured x nodes that do not include node A or B

compared to combinatorial design. However, for security enhancement, some locations on the 3D space may be kept empty while assigning keys to those locations, and this will necessitate more colluding routers to compromise all the secret keys of an MR [25]. As the mesh enterprise networks are deployed in closed environments (offices, shopping malls, etc.), and the mesh network operator has full control over the MRs, it is reasonable to expect that a large-scale attack is difficult to launch in the network. So, the proposed scheme can be used in mesh enterprise network scenario.

If routers are designed to be compromise-tolerant, then to get all the keys assigned to an MR of a particular location, an attacker has to capture all the MCs under that MR. Hence, by assigning only a subset of MR's key set K_{ijk} to its subordinate MCs where $\bigcup_{i=1}^{n} \zeta_i \neq K_{ijk}$, enhanced security may be achieved.

Symmetric key-based router–router and client–router SKE technique has been presented in Section 4.3. Secure communication is achieved, exploiting the use of the session key since a session key is an ephemeral secret, i.e., one whose use is restricted to a short time period such as a single session, after which all traces are eliminated. For a particular session, all data are encrypted with the session key to achieve data confidentiality and a MAC is generated to achieve message integrity, as shown in Eqs. 8 and 12, respectively. Replay attack is also protected as the time stamp is used in deriving the session key in client–router SKE as shown in Eqs. 9, 10, and 11. Moreover, as a second line of defense, an efficient algorithm (WSRT) is presented to deal with the malicious clients.

Storage overhead: According to key distribution, each MR is preloaded with m^2 keys and each MC has to store m^2/n keys. Also, each MR needs to store all the ID of other routers and its subordinates' (MCs') ID.

Computation overhead: To find common keys between two MRs, it requires solving the system of linear equations in Eq. 5, which needs $O(m)$ operations, where m is the size of the cubic matrix. To compute a session key from those common keys, they use simple $m-1$ exclusive OR operations, as shown in Eq. 8. To derive a session key between an MR and MC, each has to compute only two MAC and two symmetric key operations and generate a single nonce, as shown in Table 2 (Eqs. 9, 10, and 11). Finally, to run the detection algorithm, each router requires $O(n)$ computations, where n is the number of clients under each router.

Communication overhead: No message transmission is required to establish a session key between any two communicating MRs since routers know their neighbors' locations during network set-up phase. Additionally, for both MC and MR, only one message transmission is required by each party (i.e., one message transmitted by the MC to the MR and one message transmitted by the MR to the MC) to derive a session key between them as shown in Table 2 (Eqs. 9 and 10). This makes the protocol efficient since communication overhead is the minimum incurred by the security scheme for the router–router (mesh infrastructure) and for the client–router SKE.

Table 2 Computation and communication overhead for the SKE protocol

		Comp.				Comm.
		Symm. key oper.	MAC oper.	nonce	XOR oper.	no. of msg.
MR–MR	MR	0	0	0	$m-1$	0
	MC	–	–	–	–	0
MC–MR	MR	2	2	1	0	1
	MC	2	2	1	0	1

5 Malicious client detection

5.1 Basic idea

Contention-based CSMA/CA protocols are usually adopted in mesh networks for wireless users to share a common wireless channel as mentioned in Section 1. Therefore, a greedy client can substantially increase his share of bandwidth, at the expense of the other clients, by misusing the access protocols, which unfairly occupies wireless channel and resources [6]. This can become a serious problem in Internet access hotspots where individual clients have to pay for network usage and, hence, may be motivated to cheat in order to increase their share of the medium. For example, a small back-off interval gives the corresponding client the advantages of gaining access to the wireless channel quickly. Apart from small back-off values, a malicious client can disobey the CSMA/CA protocol in other ways as well. It can choose a smaller contention window size or it may reserve the channel for a larger interval than the maximum allowed network allocation vector duration. As a result, it may gain a higher share of bandwidth by sending more packets in the network over regularly behaving honest clients. In this paper, we consider that all the clients have similar applications running and they have the same data rates, so clients attached to a router are expected to have equal shares of bandwidth. Therefore, we have designed the detection mechanism mainly by measuring the number of packets for distinguishing the clients gaining the higher share of bandwidth (by deliberately misusing the access mechanism, e.g., smaller contention window) than other clients. Our detection algorithm uses a popular distribution-free statistical test, the WSRT [16], as described in the following section.

5.2 Detection mechanism

We propose a lightweight mechanism to detect the presence of malicious client(s) in the network based on the WSRT technique [16]. The proposed detection algorithm relies on the observation that the greedy behavior of malicious client(s) may significantly decrease the bandwidth share for the other well-behaved clients in the network, as described in Section 5.1. In our approach, during the normal functioning of the network (i.e., no client is malicious), each router measures the number of packets received from each of its clients for a monitoring period T and stores them as reference values. Then, the MR periodically compares the current values against the reference values by executing the distribution free statistical test based on the WSRT technique to identify the malicious clients. We have selected the Wilcoxon test because it attains good detection rates even with a small sample set, uses paired measurements (i.e., measurements from the same samples before and after an experiment), and does not assume any underlying distribution on the measurement (e.g., normal distribution). On one hand, using a small sample set adds little computation overhead. On the other hand, the ability to use paired measurements allows MRs to use the number of packets of the clients, which is achieved by means of a statistical passive approach based on traffic monitoring. Our detection technique is distributed since MRs act as local aids in the detection of misbehaving clients. We describe the detection mechanism in the following.

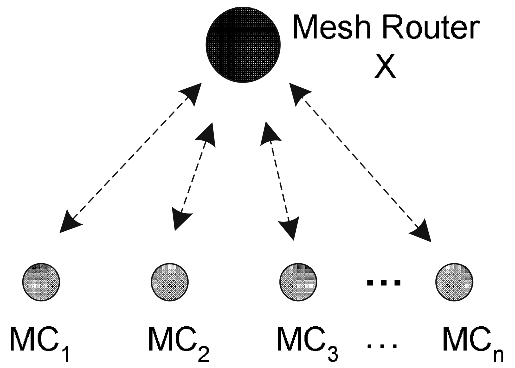


Fig. 4 Malicious client detection: there are n MCs under an MR X. Router X periodically updates its clients' information to identify malicious clients using the WSRT algorithm

Let n be the number of client nodes whose packets are received by the router X as shown in Fig. 4. The detection mechanism performed by the router X is presented in the WSRT algorithm, as shown in Table 3. Traffic traces of clients are collected (by the router X) periodically during the monitoring period T and are compared against the reference values to observe the deviation, if there is any. Since the WSRT algorithm only exploits the readily available information of the number of packets counted by the router X, it does not incur any bandwidth (communication) overhead. The computation overhead involves $O(n)$ operations that lie mainly in the WSRT procedure.

After observing any malicious behavior, a router can make a notification about the client to the WMEN operator. Upon receiving the notification, the operator can decide how to react to malicious client(s). For example, the operator can charge a penalty bill, reduce the service quality, or even completely stop the service, depending on the extent of the observed behavior and the responsiveness of the client. As a result, a malicious client will be restricted from taking the advantage at the expense of other well-behaved clients in the network.

5.3 Discussion

Our detection technique identifies the misbehaving client(s) using the number packets as the metric with the assumption that all clients have the same application running and that they have the same data rates. There might be different applications with different data rates and/or different packet lengths in the network and, hence, some clients may have more traffic compared to others. However, our detection algorithm can easily handle such cases as described in the following.

There can be different traffic classes (i.e., different applications) in the network and, hence, traffic of a certain class might generate data at a rate higher than the others. Suppose that there are C traffic classes and data rate associated with the i^{th} class (where $i = 1, 2, \ldots, C$) is R_i packets/second. We define the normalized data rate (in packets/second) of the i^{th} class as R_i/w_i, where w_i is the weight associated with the traffic class i. A higher value of the weight indicates the importance of the traffic class and, hence, a higher rate of the traffic class. We assume that weights are assigned in a way so that normalized rates are equal for all the traffic classes. In this case, the normalized data rate R_i/w_i is expected to be equal for the clients attached to an MR. So, instead of the number of packets, using the normalized data rate as the metric, the router can distinguish a

Table 3 WSRT Algorithm

1. During the normal functioning of the network (i.e., no client is malicious), router X records the number of packets it received from n MCs as $(b_1, b_2, \ldots, b_n)$ for a monitoring period T as the reference.
2. Router X periodically compares the current packet counts recorded at it as $(c_1, c_2, \ldots, c_n)$ against the reference records $(b_1, b_2, \ldots, b_n)$ using the WSRT procedure, stated below.
   a. Compute $d_i = b_i - c_i$. Exclude d_i that is 0 and order non-zero absolute values $|d_i|$ to obtain the rank r_i for each ordered $|d_i|$.
   b. Let g be the number of non-zero d_i's and I be the indicator function with value 1 and -1, compute $\mathbb{R} = \sum_{i=1}^{g} I(d_i) r_i$
   c. If there is no malicious client, the statistic $\mathbb{R}$ follows normal distribution with mean 0 and standard deviation $\sigma_{\mathbb{R}} = \sqrt{\frac{g(g+1)(2g+1)}{6}}$. Then, we can get the p value from the calculated $\mathbb{R}$ based on the expected normal distribution.
   d. Return p.
3. Finally, the decision that the client is malicious, if p is less than a given threshold.

client that accesses the medium higher than the other clients.

In another case, there can be different traffic classes with different packet lengths, for example, voice over IP (VoIP) versus streaming video. In this case, the bandwidth required for the latter will naturally be much larger than that of VoIP traffic. Suppose that there are C traffic classes and data rate associated with the i^{th} class (where $i = 1, 2, \ldots, C$) is R_i packets/second. We define the normalized data rate (in packets/second) of the i^{th} class as $(\frac{\text{packetsize}_i}{\text{Max(packetsize)}} \times \frac{R_i}{w_i})$, where packetsize_i is the length (e.g., in bytes) of a data packet of the i^{th} class, Max(packetsize) is the maximum length (in bytes) of a data packet in the network, and w_i is the weight associated with the traffic class i. Again, instead of the number of packets, using the normalized data rate as the metric, the router can detect a client that gets a higher share of bandwidth at the expense of the other clients.

5.4 Simulation and results

In this section, we evaluate the performance of the proposed detection algorithm through simulations using NS-2 [29]. We consider a network of 125 MRs uniformly located at 125 locations in a 5 × 5 × 5 matrix. There are eight MCs attached to each MR (i.e., there are total of 1,000 clients). Matrix locations are uniformly placed in 350 × 350 × 350 m terrain, where the distance between any two neighboring MRs is kept within the transmission range of each other. Transmission range is taken as 50 m for both MR and MC, and MCs are attached to their nearest MRs. We consider that all the clients always have packets (of same size) to send (i.e., all the MCs in the network are backlogged).

We examine the detection efficiency and false positive rate with the number of malicious clients varying from 5% to 30% of the total clients. The detection efficiency ϵ is defined as $\epsilon = z/Z$, where z denotes the number of malicious clients detected and Z denotes the total number of malicious clients in the network. The false positive rate Υ is defined as $\Upsilon = f/F$, where f denotes the number of legitimate clients detected as malicious ones and F denotes the total number of clients in the network. We use the commonly used confidence level of 95% for the test results and, hence, the threshold 0.05 is used in WSRT algorithm.

To implement the proposed detection mechanism in NS-2, we randomly vary contention window sizes for 5–30% of the total clients while setting that to the default value (of 802.11 medium access control layer implementation in NS-2) for the rest of the clients. Since clients with smaller contention window sizes access the medium quicker than the clients with default contention window size, they send more packets to the routers. We have used the well known random waypoint mobility model as the client mobility pattern by modifying the default implementation in NS-2. Each client is initially attached with an MR within the simulation terrain. As the simulation progresses, each client

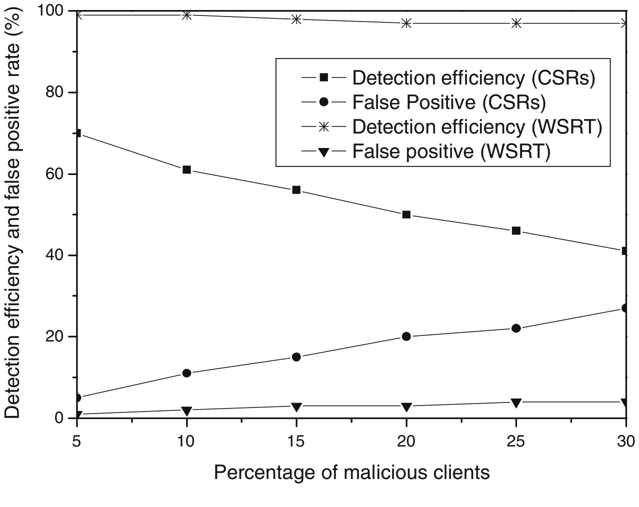


Fig. 5 Simulation results: detection efficiency and false positive rate with different percentage of malicious clients. Results are compared with the previous malicious client detection algorithm (CSRs) in [8]

pauses at its current location for a period and then randomly chooses a new location to move to and velocity between 0.2 and 0.6 m per second at which to move there. Each client continues this behavior, alternately pausing and moving to a new location (and attaches to its nearby MR), for the duration of the simulation.

Figure 5 shows the detection and false positive rates of our algorithm for different values of malicious clients. We observe that the WSRT algorithm produces a high detection rate, even when the number of attackers is large, compared to the CSRs algorithm developed in [8]. For example, the detection rate is over 98% when there are only 5% to 10% malicious clients (50 to 100 of 1,000 clients). The detection rate is more than 95% when the number of attackers is smaller than 30% (300 clients out of 1,000). The false positive rate of the WSRT algorithm also outperforms the CSRs-based algorithm, as shown in Fig. 5. As can be seen, WSRT reduces the false positive rate below 4%, while it is more than 30% in the CSRs-based algorithm when the number of malicious clients is 30%. Since malicious clients are allowed to vary the contention window size, they may exploit the medium access mechanism with some routers and behave normally with other routers. Consequently, malicious clients may maintain average correlation (calculated from the CSRs [8]) higher than the detectable threshold as explained in Section 2.1. On the contrary, with the proposed algorithm, each router independently detects misbehaving client(s) regardless of how they behave with other routers. Thus, WSRT algorithm improves the detection efficiency compared to the technique presented in [8]. Furthermore, unlike the algorithm presented in [8], detection efficiency using WSRT technique is not confined by the number of malicious clients.

6 Conclusions

In this paper, we have designed a security scheme for WMENs considering the characteristics of the network topology and communication scenarios. Through analysis, we have shown that matrix key distribution has great potential to suit mesh enterprise networks and is robust against small-scale attacks. To achieve the communications security for routers and clients, we have developed SKE protocols that require fewer communication and computation overheads. Finally, to identify malicious clients, we present a detection technique, and our simulation results show that the proposed technique achieves better detection efficiency and reduces false positive rates. In terms of future work, we intend to study, in more detail, general topology networks.

Acknowledgements This research was supported by the MKE under the ITRC support program supervised by the IITA (IITA-2008-(C1090-0801-0016)).

Dr. Choong Seon Hong is the corresponding author.

References

1. Akyildiz IF, Wang X, Wang W (2005) Wireless mesh networks: a survey. Comput Networks 47(4):445–487
2. Yang L, Zerfos P, Sadot E (2005) Architecture taxonomy for control and provisioning of wireless access points (capwap). IETF RFC 4118
3. Alam SMN, Haas ZJ (2006) Coverage and connectivity in three-dimensional networks. In: MOBICOM, Los Angeles, 23–29 September 2006, pp 346–357
4. Ben Salem N, Hubaux JP (2006) Securing wireless mesh networks. IEEE Wirel Commun 13(2):50–55
5. LAN/MAN Standards Committee, ANSI/IEEE Std 802.11 (1999) Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Computer Society, Los Alamitos
6. Radosavac S, Baras JS, Koutsopoulos I (2005) A framework for mac protocol misbehavior detection in wireless networks. In: WiSe '05: proceedings of the 4th ACM workshop on wireless security. ACM, New York, pp 33–42
7. Cagalj M, Ganeriwal S, Aad I, Hubaux JP (2005) On selfish behavior in CSMA/CA networks. In: INFOCOM, Miami, 13–17 March 2005, pp 2513–2524
8. Hamid M, Islam M, Hong CS (2008) Developing security solutions for wireless mesh enterprise networks. In: IEEE wireless communications and networking conference, 2008 (WCNC '08), Las Vegas, 31 March–3 April 2008, pp 2549–2554
9. Zhang Y, Fang Y (2006) Arsa: an attack-resilient security architecture for multihop wireless mesh networks. IEEE J Sel Areas Commun 24(10):1916–1928
10. Wu X, Li N (2006) Achieving privacy in mesh networks. In: SASN '06: proceedings of the fourth ACM workshop on security of ad hoc and sensor networks. ACM, New York, pp 13–22
11. Wu T, Xue Y, Cui Y (2006) Preserving traffic privacy in wireless mesh networks. In: WOWMOM '06: proceedings of the 2006 international symposium on world of wireless, mobile and multimedia networks. IEEE Computer Society, Washington, DC, pp 459–461
12. Tague P, Poovendran R (2007) Modeling adaptive node capture attacks in multi-hop wireless networks. Ad Hoc Netw 5(6):801–814
13. Santhanam L, Nandiraju D, Nandiraju N, Agrawal D (2007) Active cache based defense against dos attacks in wireless mesh network. In: Wireless pervasive computing, 2007. ISWPC '07. 2nd international symposium, San Juan, 5–7 February 2007
14. Li H, Xu M, Li Y (2007) Selfish mac layer misbehavior detection model for the ieee 802.11-based wireless mesh networks. In: Proceedings of advanced parallel programming technologies (APPT '07), vol. 4847. Springer, Berlin Heidelberg New York, pp 382–391
15. Dong J, Ackermann KE, Bavar B, Nita-Rotaru C (2008) Mitigating attacks against virtual coordinate based routing in

wireless sensor networks. In: WiSec '08: proceedings of the first ACM conference on wireless network security. ACM, New York, pp 89–99

16. Lowry R (2006) Concepts and applications of inferential statistics. Vassar College, Poughkeepsie
17. Ravelomanana V (2004) Extremal properties of three-dimensional sensor networks with applications. IEEE Trans Mob Comput 3(3):246–257
18. Bahramgiri M, Hajiaghayi M, Mirrokni VS (2006) Fault-tolerant and 3-dimensional distributed topology control algorithms in wireless multi-hop networks. Wirel Netw 12(2):179–188
19. Gupta P, Kumar PR (2001) Internet in the sky: the capacity of three dimensional wireless networks. Commun Inf Syst 1:33–49
20. Cao Q, Abdelzaher T (2006) Scalable logical coordinates framework for routing in wireless sensor networks. ACM Trans Sen Netw 2(4):557–593
21. Akyildiz IF, Pompili D, Melodia T (2005) Underwater acoustic sensor networks: research challenges. Ad Hoc Netw J (Elsevier) 3(3):257–279
22. Carle J, Myoupo JF, Semé D (2001) A basis for 3-D cellular networks. In: ICOIN '01: proceedings of the 15th international conference on information networking. IEEE Computer Society, Washington, DC, p 631
23. Decayeux C, Seme D (2004) A new model for 3-D cellular mobile networks. In: ISPDC '04: proceedings of the third international symposium on parallel and distributed computing/third international workshop on algorithms, models and tools for parallel computing on heterogeneous networks. IEEE Computer Society, Washington, DC, pp 22–28
24. IEEE 802.11s Task Group (2007) Draft amendment to standard for information technology telecommunications and information exchange between systems - LAN/MAN specific requirements - Part 11: wireless medium access control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking, IEEE P802.11s/D1.06
25. Gong L, Wheeler DJ (1990) A matrix key-distribution scheme. J Cryptol 2(1):51–59
26. IEEE Standard 802.1X-2004 (2004) Standard for local and metropolitan area networks: port-based network access control. IEEE, Piscataway
27. Ņostel J (1981) Internet control message protocol (ICMP). RFC 792
28. Çamtepe SA, Yener B (2007) Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Trans Netw 15(2):346–358
29. The network simulator - ns-2 (2003). http://www.isi.edu/nsnam/ns/index.html