This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2008 proceedings.

Developing Security Solutions for Wireless Mesh Enterprise Networks

Md. Abdul Hamid, Md. Shariful Islam, and Choong Seon Hong
Networking Lab, Department of Computer Engineering, Kyung Hee University, 449-701, Republic of Korea
E-mail: {hamid, sharif}@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract—**Our study on the deployment topology and communication characteristics of wireless mesh enterprise networks (WMENs) leads to three critical security challenges: (a) deployment of network devices are not planar, rather devices are deployed over three-dimensional space, (b) message generated/received by a mesh client traverses through mesh routers in a multi-hop fashion, and (c) mesh clients being mostly mobile in nature may result in misbehaving or spurious during communications. We address these challenges for WMENs that may be a small network within an office or a medium-size network for all offices in an entire building, or a large scale network among offices in multiple buildings. We develop a matrix key distribution technique that perfectly suits the network topology. A session key establishment protocol is presented to achieve the client-router and router-router communication security. Finally, a misbehaving client detection algorithm is developed based on the communication history. We analyze and evaluate the performance to show the suitability of our proposed security solutions.**

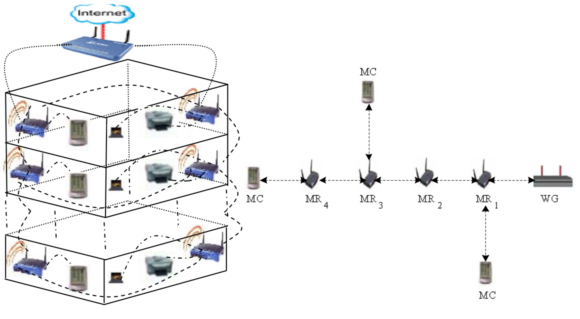
Keywords- mesh enterprise networks; key distribution; communications security; malicious client detection.

I. INTRODUCTION

Wireless mesh network (WMN) represents a paradigm shift away from the rigid, long-lead planning and implementation of the wired backbone, and toward a real-time plug-and-play deployment model that is up to the challenges of today's rapidly-changing connectivity environment. By making it possible to put Ethernet ports anywhere—easily, instantly and affordably—the wireless mesh will soon have a role to play in virtually every private and public network. Wireless mesh enterprise networks (WMENs) may be defined as a small network within an office or a medium-size 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 mesh routers, as shown in Fig.1a, Ethernet wires can be eliminated. WMNs can grow easily as the size of 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]. However, WMNs for enterprise networking are much more complicated than at home because more nodes and more complicated network topologies are involved.

Before identifying the security problems, let us sub-divide the communication scenario in a typical mesh enterprise network as depicted in Fig. 1b.

1. *Client-router*: Whenever a client wants to send/receive data, it communicates with its nearby router. We consider that mesh clients are one-hop away from their nearby routers.
2. *Router-router*: A set of stationary mesh routers form the wireless backbone of a WMEN and data must traverse using these backbone routers possibly in a multi-hop fashion.
3. *Router-gateway*: As mesh routers are connected to the wired infrastructure/Internet via wireless gateways, they must rely on the *WG* to relay their data to/from Internet.



(a) (b)

Figure 1. (a) A mesh enterpise network deployed in a multi-floored building. (b) A typical communication scenario: The communications between MC-MC and MC-WG are perfromed via MRs in a multi-hop fashion where an MC is within the transmission range of its nearby router.

In this paper, we focus on developing the security solutions for *client-router* and *router-router* communications and do not consider *router-gateway* communication security problem as strong security may be achieved with the powerful gateway.

To identify the security problems, let us present the underlying characteristics of the topology and communication scenarios of a mesh enterprise network based on Fig. 1. Fig. 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 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 [2]. Most often 2D schemes are applied in 3D scenarios ignoring the third dimension. To some

This research was supported by the MIC under the ITRC support program supervised by the IITA (IITA-2007-(C1090-0701-0016)). Dr. C. S. Hong is the corresponding author.

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 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 and any 2D model would assume that they are in the same location, and yet they are not. Therefore, a modest contribution towards ameliorating key distribution and communication security problem is crucial to suit 3D characteristics of the network topology.

Fig. 1b shows the communications between *MC-MC* and *MC-WG* are performed via *MR*s in a multi-hop fashion where an *MC* is within the transmission range of its nearby router. Mutual authentication between *client-router* and *router-router* is a pre-requisite 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 DoS attack respectively [11]. So, it is preferable to develop an authentication scheme based on symmetric key cryptography for the communication scenarios described herein.

As all the MRs are static and MCs are mobile, the network is compounded by the fact that *MC*s are dynamic in the sense they are free to join and leave at will. This will result in the possibility of some clients to be misbehaving or spurious and may impair the network from achieving its desired goal. Therefore, it is necessary to develop an efficient technique to detect misbehavior and identify the exact node to defend the network being crippled.

Specifically, the contributions that bring into focus of our work shall answer the following questions:

1. Given an enterprise mesh network as depicted in Fig.1a, how to design an efficient key distribution mechanism that suits the underlying network topology?
2. How the communications security between *client-router* and *router-router* can be achieved with the proposed key distribution mechanism?
3. Considering the mesh clients are mobile (i.e., free to join/leave), how to develop a detection strategy to identify unpredictable presence of a misbehaving/malicious client/intruder?

We exploit the matrix key distribution concept to answer the first question. First, we provide the insight of the basic 2D matrix-key distribution technique presented in [3], then, a 3D technique is engineered to apply to mesh enterprise networks. To answer the second question, we develop a session key establishment protocol for *router-router* and *client-router* communication. For two communicating *MC*s, based on the existing communication history with a common set of routers, we develop a malicious client detection algorithm that runs in each router, and thereby we answer the last question. Throughout this paper, we use the notations shown in Table I.

TABLE I. 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 device A and B
E(K, msg)	Encryption of message *msg* with key *K*
MAC(K , msg)	Message Authentication Code using *msg* and *K*
cov(x, y)	Covariance of variable *x* and *y*
$\rho(x,y)$	Correlation between variable *x* and *y*

The rest of the paper is organized as follows. We present our security schemes in details in Section II. In Section III, we present security analysis. Section IV describes related works and Section V concludes our work.

II. SECURITY SCHEME

A. 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 either on the same row or column as n_{ij}. Hence n_{ij} gets the keys according to (1).

$$K_{ij} = \{k_{xy} \mid x = i \text{ or } y = j\} \quad (1)$$

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} which are common between A and B to compose a session key (Fig. 2).

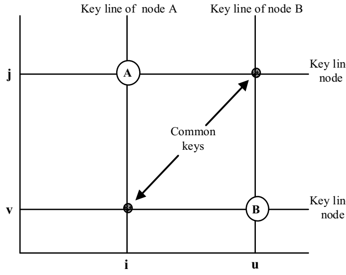


Figure 2. Conventional matrix-key distribution.

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 multi-line protocol is developed in [3] by allocating more key lines to each node instead of only two as in the basic scheme. In multi-line protocol, the key set of node n_{ij} is assigned according to (2).

$$K_{ij} = \left\{ k_{xy} \mid y - j + C_l(x - i) = 0 \bmod (m) \right\} \qquad (2)$$

where, $l = 1,2,...,t$ 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 (3).

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

where, $p, q = 1,2,...,t$ 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. We further refer to [3] for clear understanding of the basic matrix key scheme.

B. 3D Matrix Key Distribution

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 $N \leq m^3$. Each of the m^3 cells is assigned a location (i, j, k) and one secret key for each location denoted as k_{ijk} where, $i, j, k = 0,1,2,...,m-1$. Then N mesh routers are placed one in each cell with location (i, j, k). Secret keys are distributed to *MR*s and *MC*s in such a way that each *MR* or 3D location is pre-loaded with multi-plane keys and the *MC*s within its *MR* hold a distinct subset of those keys as described below.

The key set for a router is assigned according to (4) as

$$K_{ijk} = \left\{ k_{xyz} \mid z - k + C_{l_\alpha}(y - j) + C_{l_\beta}(x - i) = 0 \bmod (m) \right\} \qquad (4)$$

where, $l = 1,2,...,L$ and $C_{p_\alpha} \neq C_{q_\alpha} OR\ C_{p_\beta} \neq C_{q_\beta}$ when $p \neq q$.

The key set, K_{ijk} is a set of keys assigned to locations on L planes on the 3D matrix all passing through point (i, j, k). Any two communicating routers on the matrix, say, n_{ijk} and n_{uvw} solve $L(L - 1)(L - 2)$ linear equation groups, each of which has the form of (5).

$$\left. \begin{aligned} z - k + C_{p_\alpha}(y - j) + C_{p_\beta}(x - i) = 0 \bmod (m) \\ z - w + C_{q_\alpha}(y - v) + C_{q_\beta}(x - u) = 0 \bmod (m) \\ z - f + C_{r_\alpha}(y - e) + C_{r_\beta}(x - d) = 0 \bmod (m) \end{aligned} \right\} \qquad (5)$$

where, $p, q, r = 1,2,...,L$ and

$$(C_{p_\beta} - C_{q_\beta})(C_{q_\alpha} - C_{r_\alpha}) \neq (C_{p_\alpha} - C_{q_\alpha})(C_{q_\beta} - C_{r_\beta}) .$$

The third point (d, e, f) in (5) is calculated as $d = (i + u) \bmod(m)$, $e = (j + v) \bmod(m)$, $f = (k + w) \bmod(m)$ by the communicating routers n_{ijk} and n_{uvw}. The solution can be found easily, for example, the value of x can be calculated by (6).

$$x - 2i + u = \frac{\begin{aligned} &(C_{p_\beta}C_{q_\alpha} - C_{p_\beta}C_{r_\alpha})(u - i) + (C_{p_\alpha}C_{r_\beta} - C_{q_\alpha}C_{r_\beta}) \\ &(d - u) + C_{p_\alpha}C_{q_\alpha}(v - j) + C_{p_\alpha}C_{r_\alpha}(j - e) + \\ &C_{q_\alpha}C_{r_\alpha}(e - v) + C_{p_\alpha}(w - f) + C_{q_\alpha}(f - k) + C_{r_\alpha}(k - w) \end{aligned}}{(C_{p_\beta} - C_{q_\beta})(C_{q_\alpha} - C_{r_\alpha}) - (C_{q_\beta} - C_{r_\beta})(C_{p_\alpha} - C_{q_\alpha})} \bmod(m) \qquad (6)$$

The solutions (x, y, z) are some locations of the keys that router n_{ijk} and n_{uvw} have in common. Note that, when the size of the matrix, m is chosen to be a prime, each equation group has exactly one solution. If m is not a prime, there may exist none, one, or more than one solution [3].

From the 3D multi-plane key pre-distribution, each *MR* is pre-loaded with $L \times m^2$ keys, where L is the number of planes and m is the size of the 3D matrix. The WMEN operator may pre-distribute each MC_i within its *MR* a subset ζ_i keys from these Lm^2 keys according to (7) as

$$\zeta_i = Max\{\left\lfloor Lm^2 / n \right\rfloor, 1\} \qquad (7)$$

where, n is the number of *MC*s under each router. Note that, if $L \times m^2 \geq n$, then within a router, each of the n *MC*s has distinct set of keys.

C. Session Key Establishment (SKE)

Router-router SKE: If we carefully look at multi-plane key distribution (Section II-B), it can be seen that two routers can find common keys without requiring any exchange of messages, rather they need to compute a linear equation groups provided that each router knows its neighbor routers' location information. Here, we show that two communicating routers can establish a session key from these common keys using any pre-defined secure function without any message exchange. For example, they can use a subset of common keys. Suppose two routers MR_u and MR_v have a subset f, of common keys and they may compute a session key using simple exclusive *OR* operations as (8).

$$K_{(MR_u, MR_v)} = k_1 \oplus k_2 \oplus ... \oplus k_f \qquad (8)$$

Then using this session key, both the routers may exchange message securely and verify message integrity. For example, router MR_u sends a message *msg* to MR_v according to (9).

$$MR_u \rightarrow MR_v : MAC(K_{(MR_u, MR_v)}, msg), E(K_{(MR_u, MR_v)}, msg) \qquad (9)$$

Client-router SKE: A mesh client MC_i may establish pair-wise session key with its corresponding MR_j (client i under router j) using one of its ζ_i keys prior to sending messages. To establish a session key, MC_i unicasts a key negotiation message to communicate with MR_j as (10).

$$\begin{aligned} &MC_i \rightarrow MR_j : \\ &ID_{MC_i}, ID_{k_i}, nonce_{MC_i}, MAC(k_i, ID_{MC_i} \parallel ID_{k_i} \parallel nonce_{MC_i}) \end{aligned} \qquad (10)$$

MR_j authenticates MC_i by checking *MAC* and accordingly unicasts a message to compose a session key with the shared key $k_i \in \zeta_i$ as (11).

$$\begin{aligned} &MR_j \rightarrow MC_i : \\ &ID_{MR_j}, nonce_{MR_j}, MAC(k_i, ID_{MR_j} \parallel nonce_{MR_j}) \end{aligned} \qquad (11)$$

Session key $K_{(MR_j, MC_i)}$ between MR_j and MC_i is derived as (12).

$$K_{(MR_j, MC_i)} = MAC(k_i, nonce_{MR_j} \parallel nonce_{MC_i}) \qquad (12)$$

Then using this session key, both the router and the client may exchange message securely and verify message integrity. For example, client MC_i sends a message *msg* to MR_j according to (13).

$$MC_i \rightarrow MR_j : MAC(K_{(MR_j, MC_i)}, msg), E(K_{(MR_j, MC_i)}, msg) \qquad (13)$$

D. Malicious Client Detection

We develop a preventive solution to deal with the colluding actions taken by the malicious intruder, i.e., mesh clients. Fig. 3 shows the communication scenario between two *MC*, *p* and *q* via a common set of routers. Common set is chosen based on the close relationship with the two communicating clients. For example, all the past messages between client *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 client *p* and *q* and a decision whether client *q* is malicious or not is sent to client *p* at the time client *p* wants to communicate with *q*.

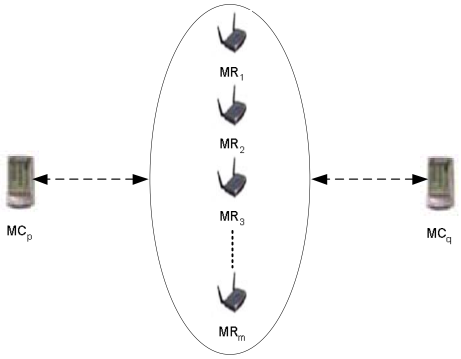


Figure 3. A communication scenario between mesh clients *MCp* and *MCq* via common set of mesh routers R_1, R_2, …, R_m.

Suppose $M = \{R_1, R_2, R_3, \ldots, R_m\}$ is a common set of routers through which clients MC_p and MC_q exchange messages. Let us define two set trust values $T_p = \{t_1, t_2, t_3, \ldots, t_m\}$ and $T_q = \{t_1, t_2, t_3, \ldots, t_m\}$ for the two clients MC_p and MC_q respectively. Then, individual trust between MC_p and its common communicating set *M* is evaluated as $t_1 = (S_{pR1} - F_{pR1}) / (S_{pR1} + F_{pR1})$, $t_2 = (S_{pR2} - F_{pR2}) / (S_{pR2} + F_{pR2})$,…, $t_m = (S_{pRm} - F_{pRm}) / (S_{pRm} + F_{pRm})$. Similarly, individual trust between MC_q and *M* is evaluated as $t_1 = (S_{qR1} - F_{qR1}) / (S_{qR1} + F_{qR1})$, $t_2 = (S_{qR2} - F_{qR2}) / (S_{qR2} + F_{qR2})$,…, $t_m = (S_{qRm} - F_{qRm}) / (S_{qRm} + F_{qRm})$. Here, *S* and *F* denote the individual rate of legitimate and malicious messages in communicating with the common set *M*. Then we calculate the correlation ρ according to (14) as

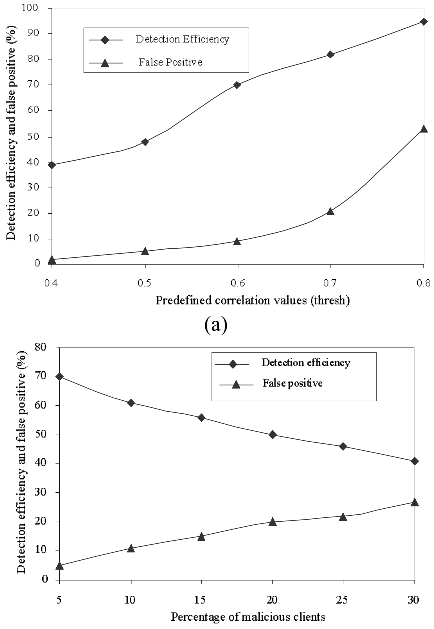
$$\rho(T_p, T_q) = cov(T_p, T_q) / \sigma_{T_p} \sigma_{T_q} \tag{14}$$

where, σ_{T_p}, σ_{T_q} are the standard deviations of client *p* and *q*, respectively. Based on this correlation value, a decision is made whether a client is malicious or not. *Algorithm 1* depicts the detection procedure.

Simulation Results: We evaluate the performance of *Algorithm 1* through simulations. We consider networks of 125 mesh routers uniformly located in a 5×5×5 matrix and under each router there are 8 mesh clients. By executing *Algorithm 1*, before communicating with a client *q*, a legitimate client *p* gets the decision whether *q* is legitimate or malicious based on the previous communication history with the set of routers common to both *p* and *q*. We set legitimate and malicious message ratio as 80:20 for normal client, whereas a malicious client always sends malicious messages.

Algorithm 1 Malicious Client Detection

```
Input: Common set of routers {M} and past communication history of mesh client p and q.
Output: Decision on client q whether it is malicious or not.
Procedure:
  1. Calculate the past trust values $T_p$ and $T_q$.
  2. Divide the common set {M} and trust values $T_p$ and $T_q$ into g groups ($g \geq 1$) as $\{\{T_{p1}\},\{T_{p2}\},\ldots,\{T_{pg}\}\}$and $\{\{T_{q1}\},\{T_{q2}\},\ldots,\{T_{qg}\}\}$.
  3. Arrange the trust values according to groups as $\{\{T_{p1},T_{q1}\},\{T_{p2},T_{q2}\},\ldots\{T_{pg},T_{qg}\}$ and calculate the correlation according to Eq.14.
  4. Calculate the average correlation $\rho_{avg} = \sum_{i=1}^{g} \rho_i / g$ .
  5. Compare the correlation with a predefined threshold thresh, if $\rho_{avg} \leq$ thresh, return true, else return false.
```



(a)

(b)

Figure 4. Simulation results. (a) ε and Υ with variable threshold values. (b) ε and Υ with different percentage of malicious clients (*thresh* is set to 6.5).

Detection Efficiency: Let *u* and *v* denote the number of malicious client detected and total number of malicious clients, respectively. Then, the detection efficiency ε is defined as $\varepsilon = u / v$. And let *x* denote the number of legitimate clients detected as malicious ones and *y* denote the total number of clients. Then, false positive rate Υ is defined as $\Upsilon = x / y$. Fig. 4 depicts the simulation results. Optimal threshold value (i.e., detection efficiency is high with minimum false positive) may be found between 0.6 and 0.65 from Fig. 4a. Fig. 4b shows the efficiency and false positive rate under optimal threshold 0.65 and we conclude that our algorithm performs better when the percentage of malicious clients is smaller. So, the algorithm has its limitation as the detection efficiency gets confined by the number of misbehaving clients. As a future work, we plan to further improve this limitation by solving the problem of reducing the false positive rate while increasing the detection efficiency.

III. ANALYSIS

Security: From the key distribution, if size of the cubic matrix m is a prime and the constants are distinct, then for a particular pair of routers, there exists a number of groups of $(L-1)$ other routers who, when colluding together, will be able to compromise the session key between that pair of routers. There are a number of groups of L colluding routers that can compromise all session keys of an *MR* with any *MR*. To realize this fact, note that there exists a group of $(L-1)$ routers, each of which has a distinct key plane in common with a router A and covers another distinct key on the L^{th} plane used in the session. This group is able to compromise *A*'s particular key for that session. A group of colluding routers, one on each of the L planes through A, can compromise all *A*'s communications. However, 3D matrix key includes all the features of the 2D scheme and it allows using more keys than 2D (in 2D keys are assigned using multi-line but in 3D based approach, keys are assigned using multi-plane. For security enhancement, some locations on the 3D space may be kept empty while assigning keys to those and a WMEN operator may change/refresh the logical locations. This will necessitate more colluding routers to compromise all the secret keys of an *MR* [3].

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 *MC*s under that *MR*. Hence, by assigning only a subset of *MR*'s key set K_{ijk} to its subordinate *MC*s such that $\bigcup_{i=1}^{n}\zeta_i \neq K_{ijk}$, enhanced security may be achieved.

Symmetric key based *router-router* and *client-router* session key establishment technique has been presented in Section II-C. Secure communication is achieved exploiting the use of 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 trace of it is eliminated. For a particular session, all subsequent data are encrypted with the session key to achieve data confidentiality and a *MAC* is generated to achieve message integrity as shown in Eq.9 and 13, respectively. Replay attack is also protected as the time stamp is used in deriving session key in *client-router SKE* as shown in Eq.10, 11 and 12. Moreover, as a second line of defense, an algorithm is presented to deal with the misbehaving clients. The algorithm has better efficiency with less number of malicious clients and it is reasonable to assume that in a WMEN, number of clients is not very large.

Storage Overhead: According to key distribution, each *MR* is preloaded with $L\times m^2$ keys and Each *MC* has to store Lm^2 / n keys. For example, a matrix of size 5, and if under each router there are 8 *MCs*, then, we have $5\times 5\times 5$ = 125 routers and 1000 clients. If, L = 2 key planes are allocated, then each router gets 50 and each client gets 6 cryptographic keys, respectively.

If m is prime and $(C_{p_\beta}-C_{q_\beta})(C_{q_\alpha}-C_{r_\alpha}) \neq (C_{p_\alpha}-C_{q_\alpha})(C_{q_\beta}-C_{r_\beta})$, two different *MR*s have in common either $L(L\text{-}1)(L\text{-}2)$ or m^2 + $(L\text{-}2)(L\text{-}3)(L\text{-}4)$ or $(L\text{-}1)(L\text{-}2)^2$ distinct keys. In fact there are 3 cases: (1) if any 2 of 3 locations in (5) are not on the same plane, then two *MR*s have exactly one position in common. This is because when m is prime, 3 nonparallel planes have exactly one intersecting point. Hence, two *MR*s have exactly $L(L\text{-}1)(L\text{-}2)$ keys in common. (2) If 3 locations are on the same plane, on that plane the two *MR*s have m^2 keys in common. Other than these, they may solve $(L\text{-}2)(L\text{-}3)(L\text{-}4)$ equation groups, each of which results in an intersecting location. (3) If any two locations are on the same plane, then three locations have $(L\text{-}1)(L\text{-}2)^2$ keys in common. Finally, each *MR* needs to store all the *ID* of other routers and its subordinates' (mesh clients') *ID*.

TABLE II. COMPUTATION AND COMMUNICATION OVERHEAD

		Comp.				Comm.
		Sym. Key Oper.	MAC Oper.	nonce	XOR Oper.	# of msg trans.
MR-MR	MR	0	0	0	*f*-1	0
	MC	-	-	-	-	0
MC-MR	MR	2	2	1	0	1
	MC	2	2	1	0	1

Computation Overhead: To find common keys between two *MR*s, it requires to solve linear equation groups in (5) which is $O(L^3)$ and to compute a session key from those common keys, they use simple *f*-1 exclusive *OR* operations as shown in (8). To derive a session key between an *MR* and *MC*, each has to compute only 2 *MAC* and 2 symmetric key operations and generate a single *nonce* as shown in Table II (Eq.10, 11 and 12). Finally, to run the detection algorithm each router requires $O(N^2)$ computations, where N is the number of routers. However, it reduces to $O(1)$ since the algorithm makes use of the previously calculated correlation.

Communication Overhead: No message transmission is required to establish a session key between any two communicating *MR* since routers know their neighbor's locations during network set up phase. And for both *MC* and *MR*, only 1 message transmission is required to derive a session key between them as shown in Table II (Eq.10 and 11). Hence, the protocol shows its efficiency since communication overhead is the minimum incurred by the security scheme as no message transmission is required for the mesh infrastructure (*router-router*) and only 1 message transmission required in *client-router* session key establishment.

IV. RELATED WORKS

A. *Security in WMNs*

Security is an important issue in multi-hop WMN which has given a little attention in the research community. In [11], the authors have identified the network operations that need to be secured in WMN are detecting corrupted router, securing routing protocol and enforcing a fairness metric. They also referred to adapt existing solutions proposed for ad-hoc network security. However, they ignored the class of attacks and malicious behavior of mesh clients. Zhang et al. in [12] have come up with an attack resilient security architecture for multi-hop WMNs. They have modeled WMN architecture as a credit card based e-commerce system and showed that a mesh client needs not 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 identity-based public key cryptosystem for authentication and key agreement between mesh clients and routers. Ref. [13] and [14] addressed the issue of privacy in WMN. But, 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 [15] have shown an effective way to modeling a node-capture attack in multi-hop WMN by formulating it as an integer-linear programming minimization problem. They claim that privacy-preserving key establishment protocols can help to prevent minimum cost node capture attack. In [16], 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 used most frequently used caching mechanism to identity flooding and raise an early alert to defend the attack. Our symmetric key based solutions eliminate the problem of computationally expensive public key solution and communication overhead incurred by the security scheme.

B. *3D Wireless Networks*

We briefly describe most of the existing works in 3D networks found in the literature. Detail explanation on different kind of polyhedrons and other necessary background information on 3D networks are provided in [2]. Assuming that nodes can be placed at any arbitrary locations, authors in [2] 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 [5] with various critical transmitting/sensing ranges for connectivity and coverage in 3D wireless sensor networks. A fault tolerant topology control algorithm is presented in [6] for a multi-hop wireless networks by varying the transmission power at each node. Each node decides on 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 are obtained in [7] and authors have shown that it has higher capacity than 2D networks. Authors conclude that wireless network connecting fewer numbers 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 coordinates based routing is presented in [8] and it is shown to be efficient in that it needs only one-hop neighborhood information and not two. Akyildiz et al. [4] 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. In cellular mobile networks [9] and [10], both studied 3D cellular networks; each cell is represented as rhombic dodecahedron in [9] and hexagonal prism shaped cells are used in [10]. Both the works focused on to extend the standard concept of planar cellular networks into space. To the best of our knowledge, no security solution is proposed for 3D networks and we develop a security scheme for such a network especially on WMEN.

V. Conclusion

In this paper, we have taken an exploratory foray into picking the security solutions for a mesh enterprise network employing symmetric cryptographic primitives. Depending on the characteristics of the network topology and communication scenarios, suitable key distribution, secure communication and malicious client detection techniques are developed. However, we realize that there is much more work to do. We plan to run the experiment on the 3D topology that has been taken into consideration in this paper. We also like to focus on the re-keying/security association issues when a client moves from one mesh router to another (handover). Finally, we intend to delve into the issue of end-to-end delay incurred by the proposed solutions as this will play an important role in the choice of right security solutions.

References

[1] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless Mesh Networks: A Survey,” Computer Networks (Elsevier), 47(4), 2005, pp. 445-487.

[2] S. M. Nazrul Alam and Zygmunt Haas, “Coverage and Connectivity in Three-Dimensional Networks,” in Proc of ACM MobiCom, 2006.

[3] Li. Gong, and D. J. Wheeler, “A Matrix-key Distribution Scheme,” Journal of Cryptology, 1990, vol. 2, pp. 51-59.

[4] Akyildiz, I.F., Pompili, D., Melodia, T., “Underwater Acoustic Sensor Networks: Research Challenges,” Ad Hoc Networks Journal, (Elsevier), March 2005.

[5] V. Ravelomanana, “Extremal properties of three-dimensional sensor networks with applications,” IEEE Transactions on Mobile Computing 3 (3), 2004, pp. 246–257.

[6] M. Bahramgiri, M. Hajiaghayi., and V. S. Mirrokni, “Fault-Tolerant 3-Dimensional Distributed Topology Control Algorithms in Wireless Multi-hop Networks,” in Wireless Networks, vol. 12, no.2, pp. 179-188, April, 2006, Springer Netherlands.

[7] P. Gupta and P.R. Kumar, “Internet in the Sky: The Capacity of Three Dimensional Wireless Networks,” Comm. in Information and Systems, vol. 1, pp. 33-49, 2001.

[8] Q. Cao and T. Abdelzaher, “Scalable Logical Coordinates Framework for Routing in Wireless Sensor Networks,” ACM Transactions on Sensor Networks, Vol. 2, No. 4, November 2006, pp. 557–593.

[9] J. Carle, J.F. Myoupo, and D. Semé, “A Basis for 3-D Cellular Networks,” in Proc. of the 15th International Conference on Information Networking, 2001.

[10] Catherine Decayeux and David Semé, “A New Model for 3-D Cellular Mobile Networks,” in Proc. Of ISPDC/HeteroPar 2004.

[11] N.B.Salem, H.P. Hubaux, “Securing wireless mesh networks,” IEEE Wireless Communications, April, 2006. pp. 50-55.

[12] Y. Zhang, Y. Fang, “ARSA: An attack resilient security architecture for multihop wireless mesh network,” IEEE Journal on Selected Areas in Communications, vol.24. no.10, October, 2006. pp. 1916-1928.

[13] X.Wu , N. Li, “Achieving privacy in Mesh Networks,” in proceedings of SASN’06, pp- 13-22, Oct. 30, 2006.

[14] W. Taojun, X. Yuan and Y.Cui, “Preserving traffic privacy in Wireless Mesh Networks,” in prod of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM’06).

[15] P. Tague, R.Poovendran “Modeling Node Capture Attacks in Multi-hop Wireless Networks,” Ad Hoc Networks, vol. 5 issue 6, August 2007, pp. 801- 814.

[16] Santhanam, L., Nandiraju, D., Nandiraju N., Agrawal D.P., “Active Cache Based Defense against DoS Attacks in Wireless Mesh Network,” 2nd International Symposium on Wireless Pervasive Computing, ISWPC '07, 5-7 Feb. 2007, pp. 419-424.