Security Framework for Hybrid Wireless Mesh Protocol in Wireless Mesh Networks

Mallikarjun Avula[1], Sang-Gon Lee[2], and Seong-Moo Yoo[1]
[1]Department of Electrical and Computer Engineering, The University of Alabama in Huntsville, Huntsville Alabama, 35899 – USA
[e-mail: {ma0004, yoos}@uah.edu]
[2]Department of Ubiquitous IT, Division of Computer & Information Engineering, Dongseo University, Busan, 617-716 – Korea
[e-mail: nok60@dongseo.ac.kr]
*Corresponding author: Seong-MooYoo

Received November 23, 2013; revised March 17, 2014; accepted May 15, 2014; published June 27, 2014

Abstract

Wireless Mesh Networks (WMNs) are emerging as promising, convenient next generation wireless network technology. There is a great need for a secure framework for routing in WMNs and several research studies have proposed secure versions of the default routing protocol of WMNs. In this paper, we propose a security framework for Hybrid Wireless Mesh Protocol (HWMP) in WMNs. Contrary to existing schemes, our proposed framework ensures both end-to-end and point-to-point authentication and integrity to both mutable and non-mutable fields of routing frames by adding message extension fields to the HWMP path selection frame elements. Security analysis and simulation results show that the proposed approach performs significantly well in spite of the cryptographic computations involved in routing.

Keywords: Wireless mesh network, hybrid wireless mesh protocol, routing frame, mutable field, non-mutable field.

Sang-Gon Lee's work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant Number: 2012-0002273).

http://dx.doi.org/10.3837/tiis.2014.06.010

1. Introduction

Wireless Mesh Networks (WMNs) have surfaced as one of the key technologies for next-generation wireless networking because of their apparent advantages over other wireless networks. Nodes in a wireless mesh network possess the capabilities of dynamic self-organization and self-configuration thereby, automatically establishing an ad hoc network yet maintaining mesh connectivity. The capabilities of ad hoc networks are diversified by mesh networks by bringing many advantages such as low cost, simplified network maintenance, robust and reliable coverage, etc. WMNs are being heavily commercialized in application areas such as broadband home and community networking, automation, metropolitan area and enterprise networking.

The IEEE 802.11s standard [13] provides a security mechanism known as Simultaneous Authentication of Equals (SAE), which uses finite field cryptography, using which the nodes authenticate each other with a password. However, this scheme provides authentication for nodes and not for routing protocols. Layer 2 (data link layer) routing is introduced in 802.11s standard which uses a default routing protocol known as Hybrid Wireless Mesh Protocol (HWMP) which uses MAC (medium access control) addresses instead of IP addressing scheme while routing. HWMP is based on Ad hoc On-demand Distance Vector (AODV) routing protocol [17] and works in either proactive or on-demand mode. The focus of research in this paper is based on securing the standard HWMP [7].

The wireless medium as well as the non-infrastructure nature of WMNs makes them increasingly vulnerable to a number of attacks. In the wireless case, an intruder can easily eavesdrop on the ongoing traffic. Since there is no centralized infrastructure, it is very difficult to have a key distribution center or a trusted certification authority to provide cryptographic keys and digital certificates to help nodes authenticate themselves. Attacks on wireless mesh routing protocols generally fall into routing-disruption attacks and resource consumption attacks. In the former case, the attacker attempts to cause legitimate data frames to be routed in dysfunctional ways. A good example for a routing-disruption attack is a scenario where an attacker induces forged routing frames which create a sort of routing loop and thus, making the frames to travel through the nodes in a cycle and preventing them from reaching their destinations resulting in energy and bandwidth consumption. In the latter case, the attacker may inject frames into the network in an attempt to exhaust network resources, such as bandwidth, or to exhaust the resources of a node such as computation power or memory storage. Research [19] shows that HWMP is vulnerable to several routing attacks such as wormhole attacks, routing disruption attacks, flooding attacks, etc. These attacks target the mutable fields of the frames exchanged in this protocol which change at every intermediate node and are prone to modification by malicious nodes.

The route discovery process in HWMP begins with a source mesh station broadcasting path request (PREQ) frames in an attempt to find a path to the destination. These PREQ frames contain two types of fields: mutable and non-mutable. Mutable fields in these frames such as TTL, hop-count and metric, change from hop to hop while non-mutable fields stay the same all the way from the source to the destination. It is challenging to authenticate mutable fields when compared to non-mutable fields because every intermediate mesh node that receives the frame

has to verify the integrity of the mutable fields followed by appending some authentication information for further propagation. Several internal attacks can be performed due to the lack of proper security framework for mutable and non-mutable fields. The motivation of this paper is to provide a secure framework for HWMP such that it provides end-to-end as well as point-to-point authentication and integrity security features for both mutable and non-mutable fields by employing cryptographic techniques which are efficient in terms of computation complexity and state-of-the-art in terms of robustness.

The primary contribution of this paper is to propose a security framework of the routing protocol which provides and ensure end-to-end as well as point-to-point authentication and integrity to both mutable and non-mutable fields of the routing frames of HWMP by adding message extension fields to all five HWMP path selection frames (path request, path reply, root announcement, path error, and gate announcement) elements. Existing schemes published in literature (described in the next section) cover a part of the security, either internal or external attacks, either mutable or non-mutable fields, either end-to-end or point-to-point authentication.

The rest of the paper is organized as follows. Section 2 provides a summary of previous studies on securing HWMP. In section 3, the overview of HWMP is provided. Also, a system model, which includes both network model and attack model, is outlined as well. The proposed security framework for HWMP is discussed in section 4 which also describes the enhancements to the existing HWMP to protect the fields in the routing frames. In section 5, the effectiveness of the proposed scheme is shown through a heuristic security analysis. Performance evaluation with simulation results is detailed in section 6. Section 7 provides the conclusion for the proposed work.

2. Related Work

Prior research exists on securing the layer-2 routing protocol HWMP. Islam et al. [6] proposed secure HWMP (SHWMP), a routing protocol which utilized the existing key hierarchy of 802.11s, identified the mutable and non-mutable fields in the routing message, protected the non-mutable part using symmetric encryption and authenticated mutable information using Merkle tree. The authors discussed the possible attacks that can be launched in HWMP for path selection. However, SHWMP does not address internal attacks.

Ben-Othman et al. [18] proposed a security mechanism based on the Identity-Based Cryptography (IBC) to secure HWMP. A media access control (MAC) address is used as the public key of the path request and path reply messages that contain mutable fields. Both internal and external problems are identified that exist in HWMP. Ben-Othman and Benitez [20] implemented the ECDSA (elliptic curve digital signature algorithm) technique to provide security in HWMP, namely, path request and path reply message. Here, only mutable fields are considered. These two schemes have no end-to-end and point-to-point integrity service for non-mutable fields. Both schemes require a private key to sign the mutable fields and public keys are distributed for signature verification. ECDSA-HWMP requires the transmission of a digital certificate to the station verifying the signature, but having a certification authority is not practical in WMNs.

Watchdog-HWMP [22] discusses a scheme for detecting illogical changes in the mutable fields and incorporates a forgery detection mechanism. In this scheme, when the stations

transmit the path request frames, they will receive the path requests propagated by their neighbors. Therefore, the transmitting station can check to see if the mutable fields are modified correctly and detect any changes which do not make sense. This method provides a watchdog monitoring of the mutable fields but cannot detect illegal modification of non-mutable fields.

Tan et al. [19] discussed the various kinds of attacks on HWMP and then listed out the vulnerabilities based on those attacks. The paper also investigated more on protecting routing messages than the data messages. Several security requirements were determined based on this analysis of these vulnerabilities. Several existing security protocols were analyzed based on the security requirements and compared in terms of quantitative complexity. General recommendations were made for a secure version of HWMP based on their security analysis.

Since these existing schemes cover a part of the security, either internal or external attacks, either mutable or non-mutable fields, either end-to-end or point-to-point authentication, there is a need to combine all issues in a combined framework. Thus, we propose a combined security framework in Section 4. In our research efforts, we will keep the usage of signature schemes to the minimum extent possible thereby, reducing the computation complexity in the mesh nodes.

3. HWMP Overview and System Model

HWMP is the default frame routing protocol for the mesh points as mandated by the IEEE 802.11s draft specification. It is a combination of reactive (or on-demand) and proactive routing which gives the mesh points the added advantage of discovering the best routes. The primitives of HWMP are derived from the AODV routing protocol which can operate in two modes. *On-demand mode* is useful for the mesh points as it enables peer-to-peer route communication in the absence of root node configuration or even when there is a root node in certain circumstances. In *proactive mode*, mesh points maintain routes to the root stations and a routing table is maintained based on the distance vectors. The two modes can act in conjunction with each other as they are not exclusive in nature. HWMP being a hybrid of reactive and proactive elements of routing enjoys the best features of each routing protocol discussed earlier. It creates and stores routes to gateway and root stations proactively while uses on-demand routing for establishing peer-to-peer communication [10].

In the path discovery process of HWMP, four different frames are involved which include Path Request (PREQ), Path Reply (PREP), Root Announcement (RANN) and Path Error (PERR). Similar to RANN, there exists another frame known as Gate Announcement (GANN) which is used by a gate node to announce its existence and has the exact same format as RANN. The HWMP frame formats are shown in **Fig. 1**. These frames have several fields which are divided into two categories: Mutable Fields (MFs) and Non-Mutable Fields (NMFs). This categorization of the fields helps understanding the security issues related to HWMP better. The MFs contain information that gets updated at every hop by the intermediate nodes. On the other hand, the NMFs contain information that remains unchanged from source through destination and this information is not supposed to be modified by any intermediate node. Before transmission, these frames are encapsulated with the standard wireless MAC header (not shown in **Fig. 1**) that contains the MAC addresses of the transmitter and receiver.

3.1 HWMP Security

Generally, routing protocols are vulnerable to both external and internal attacks. External attacks are launched by intruders who are not authorized users of the network. For example, an intruding node may eavesdrop on the frames and replay those frames at a later point of time to gain access to the network resources. Internal attacks are launched by already authenticated nodes within the network but are compromised either due to collusion or any other reason.

External attacks in the WMN can be prevented by implementing security services such as Simultaneous Authentication of Equals (SAE) and 802.1x authentication protocols. These services generate authenticated keys to authenticate frames. Integrity of the contents of the frame can be protected by including a message integrity code whereas the confidentiality can be protected by encrypting the frames with algorithms such as Advanced Encryption Standard (AES). Only link-to-link based security services are required to protect from the external attacks.

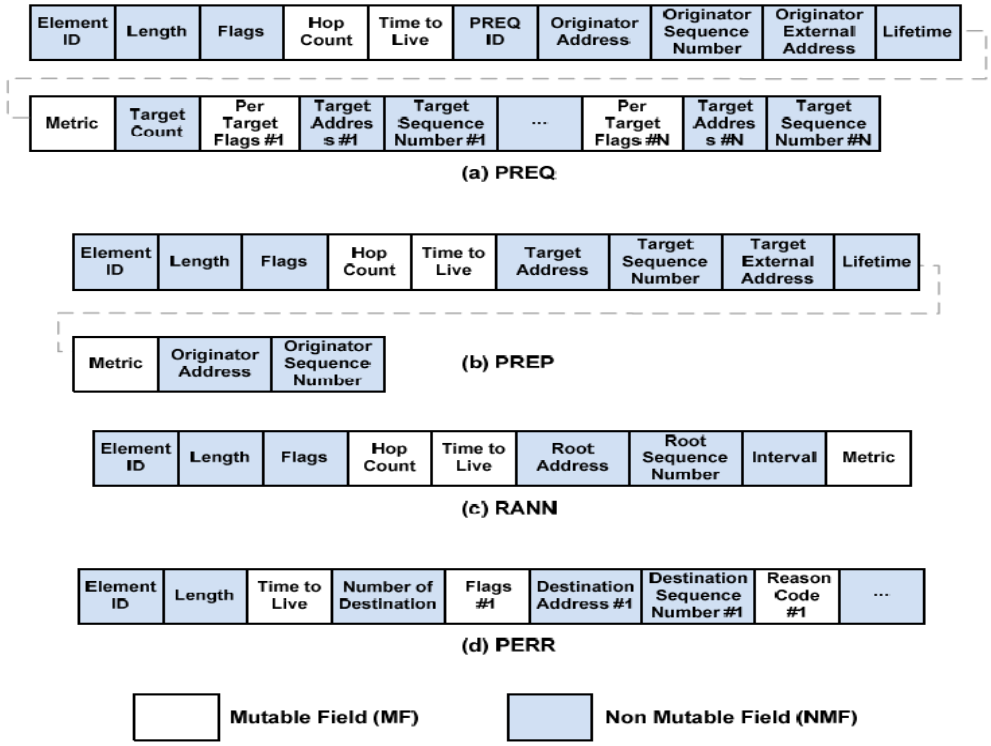

Fig. 1. HWMP frame fields (adopted from [19])

However, there is a great need to protect the WMN from internal attacks which is quite a challenging task. Path diversion and impersonation attacks are general examples of internal attacks wherein malicious nodes can exploit the routing protocol such as HWMP to create a path

diversion into a black hole or pretend as the root mesh station and spy on the frames being sent by other mesh stations for route discovery.

In order to protect the nodes from internal attacks, an efficient security service is needed to detect illegal modifications of MFs in the frames. End-to-end security schemes may prevent the modification of NMFs by intermediate nodes but do not protect the modification of MFs by malicious intermediate nodes. Therefore, link-to-link security is needed to address the security concern of MFs' modification through which a receiver can verify that the frame from the sender has not been modified by attackers. In section 4, we propose a security framework which can protect both mutable and non-mutable fields of WMNs.

3.2 System Model

In this section, the network and attack models used in the design of the proposed scheme are discussed.

3.2.1 Network Model

A typical WMN architecture is considered for the proposed scheme where the network consists of a number of mesh stations which have the mesh network capabilities and are typically routers. These mesh stations with access point functionality, known as Mesh Access Points (MAPs), can allow mesh clients to connect to the Internet through them. Mesh Portal (MP) acts a gateway between the WMN and other 802.11 networks. The WMN in the proposed scheme is modelled as an undirected labeled graph *G(V, E)*, where *V* is the set of vertices and *E* is the set of edges (links) of the graph. An edge is considered to exist between two mesh stations if the two stations are within the communication range of each other. Each station in the network is considered as a vertex of the graph and the communication links between the nodes are assumed to be bidirectional in nature.

3.2.2 Attack Model

In the design of the proposed scheme, an active-x-y attacker model [23] is used wherein an active adversary controls *x* adversarial nodes and uses *y* compromised identifiers. The attacker in consideration for the current scheme is an active-1-1 attacker. The communication capabilities of the attacker are assumed to be comparable to those of an average node in the WMN. This means that an attacker will only be able to hear the frames that are transmitted by neighboring mesh stations. Similarly, any frames transmitted by the attacker will only be heard by its neighboring mesh stations.

4. Proposed Security Framework for HWMP Protocol

To address the security concerns discussed in the previous section, the following security framework is proposed. The framework is divided into two parts: i) addressing the security of NMFs and ii) addressing the security of MFs. NMFs of the HWMP frame remain constant from the source node to the destination node in a WMN.

4.1 Routing Message Extension Fields

The most important security feature of a path discovery process is to use cryptographic methods and provide authentication of NMFs and MFs of the frame. This is accomplished by adding message extension fields to the HWMP path selection frame elements such as PREQ, PREP, GANN, RANN and PERR. The mesh station receiving the frame will be able to identify if the frame is accompanied by an extension by observing the flags field of the corresponding type of element. For example, PREQ element format has Flags field which is 8 bits long (B0:B7). Bits B3-B5 and B7 are reserved in general and thus, can be used in our proposal to notify the receiver of the existence of an extension field to the incoming frame. Similarly, PREP and PERR elements have Flags field which has B0-B5 and B7 bits reserved which can be used for the same purpose. Also, RANN and GANN elements have B1 through B7 and B0 through B7 bits reserved, respectively, that can be used for notification of message extension field.

Table 1 lists the HWMP routing message extension fields proposed in this paper. PREQ, PREP and RANN message extensions are the same as listed in the table. PERR message extension is the same as PREQ message extension except that PNM, Top Hash, and Hash fields are not required. GANN message extension is the same as PREQ message extension except that PNM is not required. The extension fields are used in route discovery and route maintenance.

Table 1. Proposed HWMP routing message extension fields

Name	Length (bytes)	Description
Type	1	1 – PREQ, 2 – PREP, 3 - PERR, 4 - RANN, 5 - GANN
Length	1	Length of type specific data, not including Type and Length fields
Reserved	2	For future use
PNM	4	Previous node metric
Top Hash	20	The top hash for the hop count authentication.
Hash	20	The hash corresponding to the actual hop count.
NMF Sign	60 + 3bits	The signature for NMFs
HMAC	20	HMAC for MFs

4.2 Non-Mutable Field (NMF) Protection

For safeguarding the NMFs of HWMP routing frames, we consider efficient Elliptic Curve Cryptography (ECC) based online/offline identity (ID) based signature scheme [1, 9] which does not require any certificate attached to the signature for verification, and does not require any pairing [8] operation in either signature generation or verification. The usage of ID based setting eliminates the requirement of attaching a certificate to the signature for verification purposes. Online/offline signature generation significantly reduces the computation cost and storage requirement involved in the generation of signatures. The signature generation process here involves two phases.

The first phase is the offline phase which is performed offline, say at the root mesh node, without the knowledge of the signed message. More importantly, this offline signing algorithm does not require any secret key information. It can be pre-computed by a private key generator [12]. The offline pre-computed information in this scheme can also be re-used unlike all other

previous online/offline signature schemes which allow only one-time usage. This eliminates the requirement for the signer to execute the offline phase every time a new message needs a signature. This is a great advantage in WMN environments as the offline information can be hard-coded to the mesh node in the manufacturing or setup stage. It can eliminate any communication between the mesh node and the root node for the offline signing, which is considered as a costly factor in the WMN. This makes this ID based online/offline signature scheme a suitable candidate for signing the NMFs of a HWMP frame in resource-constrained environments, such as a WMN, and secure against existential forgery when compared to other ID based online/offline signature schemes used for secure routing. The second phase is the online phase which is usually very fast and is performed online at the mesh station making it feasible to run this phase on resource-constrained hardware in a WMN environment.

The length of this (pre-computed) offline information (can be considered as public parameters) is about 160–bit prime modulus group elements. It may be considered long for signing a few messages. However, if the mesh station requires signing a thousand, or even a million of messages, these 160-bit group elements are just negligible when compared to those messages. Thus, this scheme is scalable for large scale networks.

For implementation of this scheme on the mesh nodes, ECC is employed due to the small key size and low computational overhead. ECC primitives in MIRACL library [14] with 160-bit key size are used. Although the normal size of the signature is 120 bytes, it can be split into two phases instead of using the entire signature every time. This is possible because *R*, a part of the signature, will be constant for all the signatures generated by a particular mesh node and therefore, can be sent once at the beginning of the communication. In the first phase, the size of the frame is 40 bytes (R = 40 bytes) and in the second phase, the size of the frame is 98 bytes (Y = 40 bytes, Z = 20 bytes, Payload = 37 bytes and another 3 bits which serve as sign identification bits for R, Y and Z when using point compression technique [21]). Payload consists of the NMFs of the HWMP PREQ frame and the size of the payload may vary between 37 to 252 bytes depending on the number of destinations in the PREQ frame.

These fields need to be provided with end-to-end security from the source node to the destination node from illegal modification by intermediate nodes. In this case, end-to-end security is sufficient because these fields do not change from hop to hop and therefore, this offline/online signature scheme can be used to sign these fields by the source node requesting the route and can be verified by the destination node to ensure the integrity of the NMFs.

Using an ID based offline/online signature scheme detects the illegal modification of NMFs of HWMP frames made by malicious intermediate nodes and thus, it avoids potential internal attacks. Therefore, this scheme provides integrity assurance of NMFs from the source node for the intermediate nodes on the transmission path to protect NMF modification attacks.

4.3 Mutable Field (MF) Protection

For safeguarding the MFs of HWMP routing frames, we use Multi-Source Broadcast Encryption (MSBE) [2, 3]. Also, we consider different schemes for path request and path reply frames. In order to prevent node deletion attacks by malicious nodes deliberately shortening the paths, two-hop authentication can be utilized. However, considering a route Y → W → X → Z, a malicious node X in the network might re-broadcast a route request frame coming from its

two-hop neighbor Y through the node W without incrementing the hop count and thus falsely portraying to the next node Z that Y is a one-hop neighbor of X. To avoid this, Z must know the one-hop neighbors of X to ensure that Y is not a one-hop neighbor of X. Also, two-hop authentication demands substantial overhead as it requires the nodes to maintain a group secret with their corresponding two-hop neighbors. Therefore, an efficient scheme is required that can detect the modifications made by non-colluding malicious nodes and at the same time provide two-hop authentication with just the available one-hop neighborhood information. We use Broadcast Encryption (BE).

One of the most efficient ways to protect the MFs in PREP frames from replay attacks is to make use of a non-interactive key agreement scheme [5]. The very nature of such schemes does not involve any interaction between any two participating mesh stations and therefore, there is no exchange of frames between them. Each mesh station will compute the mutual agreement key on its own without requiring any information from the other station.

For path request phase, a MSBE scheme using probabilistic key distribution is considered which enables multiple sources to broadcast secrets without the use of asymmetric cryptographic primitives. BE provides a means of establishing shared secret between privileged nodes among a set of nodes, whereas the remaining nodes are not provided with the secret and referred as revoked nodes. The strategy behind most probabilistic key pre-distribution schemes is to allocate a subset of keys to each node in the network from a pool of keys which are chosen by the key distribution center.

For path reply phase, the destination node already knows the route back to the source node and thus, does not have to broadcast the path reply frame. Instead, the destination would unicast the frame to the source through the intermediate nodes. Since there is no broadcasting involved here, the usage of BE seems unnecessary. One of the most basic problems in cryptography is the key distribution of frequently changing random keys used in algorithms based on symmetric encryption to protect the integrity of the communication. An example of such a situation is when two parties X and Y who want to compute a shared key K_{XY} to be used to encrypt the data transfer. In order to authenticate the MFs in the path reply frame, an identity based non-interactive key agreement scheme [5] can be employed which requires only the identity information of the mesh nodes to encrypt the communications. In this scheme, no extra public key data is needed and no interaction is required between the nodes to derive the mutual key.

Moreover, in the path reply phase, the intermediate nodes are not broadcasting the frames where a one-hop group key is used to secure the frame. Therefore, there is scope for using a scheme where minimum keys are utilized for authentication. This is the significance for using this non-interactive scheme as it greatly reduces the requirement of computation time and storage of keys in a mesh station because the two communication nodes do not interact. This is a great advantage for resource-constrained environments such as the WMN. Each node is assumed to have a unique ID and a unique secret that is not shared with any other node. Two nodes that wish to authenticate each other would use this secret to derive a mutual key to encrypt the communication. It is also assumed that a trusted authority (TA) is responsible for generating and distributing the unique secrets, derived from nodes' IDs and a master secret possessed by the TA, to the nodes. The derived mutual key is unknown to any other node besides the ones participating in the authentication. This can be a huge advantage to WMNs as this avoids the storage of large number of mutual keys by a node.

4.4 Route Discovery

4.4.1 Path Request Phase

In the following scenario, consider a source node *S* generates a PREQ frame to find a route to the destination node *D* through nodes *A*, *B* and *C* as shown in **Fig. 2**. *S* randomly selects an initial hash value *hash* and hashes it h_c times to get $s_{hc} = h^h{}_c(hash)$. The NMFs of the PREQ generated by the source node are signed using online/offline ID based signature scheme and are embedded in the PREQ as shown below. Since NMFs do not change at every hop, intermediate node authentication is not necessary and therefore, the source node signs the NMFs of the HWMP PREQ frame. This signature is then embedded in the HWMP message extension for PREQ and broadcasted.

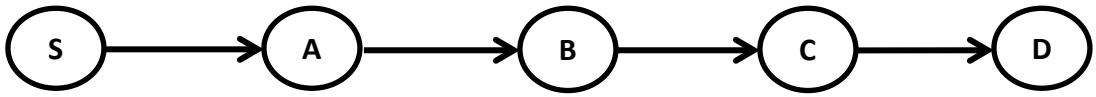

Fig. 2. PREQ flow

Source *S* originates route request as follows and broadcasts it which will be received by its one-hop neighbors. Note that the following message format only represents the HWMP message extension fields. These message extension fields are attached to the standard HWMP frames and transmitted during the route discovery process.

$S \rightarrow *:[K_s(\text{preq} \,||\, \text{NMF\_Sign} \,||\, h_c \,||\, s_{hc} \,||\, hc_S \,||\, m_S \,||\, pnm_S \,||\, s_0 \,||\, M_0 \,||\, B_S)]$

preq :The PREQ original message fields including both mutable and non-mutable fields
NMF_Sign = Signature of the NMFs of *S*
h_c = maximum hop count
s_{hc} = random value 'hash' hashed h_c times
hc_S = hop count at node *S*
m_S = airtime metric at node *S*
pnm_S = previous node metric at node *S* (0 for source node)
K_{SD} = shared symmetric key between *S* and *D*
T_S = secret chosen by *S* that is explicitly protected from all one-hop neighbors of *S*
$s_0 = h((h_c \,||\, s_{hc}), K_{SD})$
$s_1 = h(s_0)$
$M_0 = h((\{h_c \,||\, s_{hc}\}, hc_S, m_S, pnm_S, s_1), T_S)$
Bs = broadcast encryption message

K_{SD} keys are generated by using an ID based non-interactive key agreement scheme [5]. The one-hop neighbors of S will be able to decrypt the PREQ using the key K_S that was shared by *S* earlier. A neighbor node *A* will decrypt the PREQ, increments the hop count, updates metric and previous node metric, and broadcasts it by encrypting using its one-hop secret key K_A that it had shared with its one-hop neighbors as well. The previous node metric $pnm_A = m_S$. Note that it does not have access to *S*'s broadcast secret T_S.

$A \rightarrow *:[K_A(preq \parallel NMF\_Sign \parallel h_c \parallel s_{hc} \parallel hc_A \parallel m_A \parallel pnm_A \parallel s_1 \parallel M_0 \parallel S \parallel M_1)]$

$M_1 = h((\{h_c \parallel s_{hc}\}, hc_A, m_A, pnm_A, s_2), T_A)$
$s_2 = h(s_1)$
$pnm_A = m_S$

At the next hop, node *B* decrypts the message broadcasted by *A* using the one-hop secret shared by node *A*. Node *B* being the two-hop neighbor of *S* can have access to M_0 as per the broadcast encryption scheme. The integrity of PREQ can be verified by *B* and that $s_1 = h(s_0)$ is valid and node *A* did not modify the hop count, metric and PNM. The pnm_A that node *B* receives in M_0 should be equal to the m_S to ensure that node *A* did not modify the metric m_S. After the verification is successful, M_0 is stripped off by *B* and updated with M_2 for downstream verification.

$B \rightarrow *:[K_B(preq \parallel NMF\_Sign \parallel h_c \parallel s_{hc} \parallel hc_B \parallel m_B \parallel pnm_B \parallel s_2 \parallel M_1 \parallel A \parallel M_2)]$

$M_2 = h((\{h_c \parallel s_{hc}\}, hc_B, m_B, pnm_B, s_3), T_B)$
$s_3 = h(s_2)$
$pnm_B = m_A$

$C \rightarrow *:[K_C(preq \parallel NMF\_Sign \parallel h_c \parallel s_{hc} \parallel hc_C \parallel m_C \parallel pnm_C \parallel s_3 \parallel M_2 \parallel B \parallel M_3)]$

$M_3 = h((\{h_c \parallel s_{hc}\}, hc_C, m_C, pnm_C, s_4), T_C)$
$s_4 = h(s_3)$
$pnm_C = m_B$

Intermediate nodes include the previous hop identity in the frame which they are broadcasting so that the next hop can verify two-hop authentication. By doing so, the intermediate nodes will be able to cache the information about two predecessor nodes indicated in the PREQ.

Whenever a destination node receives a PREQ, the integrity of the hop count is verified by the following process: Hash function *h()* is applied maximum hop count minus number of hops (*j*) it took for the PREQ to reach the destination to the value in the most recent *hash* field value. The resulting value should be equal to the value in the s_{hc} field, $h^{h_c-j}(s_j) \stackrel{?}{=} s_{hc}$. When PREQ reaches *D* within the four hops, it is verified by the destination that s_4 is consistent with the commitment s_{hc} signed by the source and the hop count indicated in the PREQ, i.e., the destination node will verify $h^{h_c-3}(s_3) \stackrel{?}{=} s_{hc}$. Also, the destination node verifies the NMFs' signature.

4.4.2 Path Reply Phase

For path reply phase, message authentication code (MAC) hashing can be used in conjunction with a non-interactive key distribution scheme for distributing pairwise transient keys among the nodes [4]. MAC will be applied to MFs such as metric, hop count and a new field known was

PNM. It is to be verified that PNM is greater than metric at all times. By appropriate use of a key derivation function that takes the secret key computed above and session dependent information such as sequence number/time-to-live, a suitable session key is derived to protect PREP MFs from the modification attack by intermediate nodes.

K_{AB} = KDF(key_length,k_{AB}, session_param)

KDF = Key Derivation Function (say SHA-1, SHA-256, SHA-384, SHA-512, or SHA-3)
session_param = sequence number || time-to-live || target address

Now that the destination node has received the PREQ and is aware of the route to the source, it does not have to broadcast a route reply. The destination node would construct a PREP frame and unicast it to the intermediate node it received PREQ from as shown in **Fig. 3**.

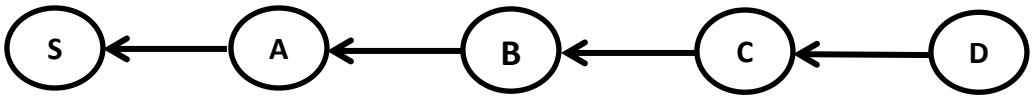

Fig. 3. PREP flow

D→C :[K_D(prep || NMF_Sign ||h'_c ||$d_{h'c}$ ||hc_D || m_D || pnm_D || d_0 || M_{DB})]

d_0 = h((h'$_c$ || $d_{h'c}$), K_{SD})
M_{DB} = h(({h'$_c$ || $d_{h'c}$}, hc_D, m_D, pnm_D, d_1), K_{DB})
d_1 = h(d_0)
h'$_c$ = hop count as indicated in PREQ from source
$d_{h'c}$ = random value 'hash' hashed h'$_c$ times
hc_D = hop count at node D
m_D = airtime metric at node D
pnm_D = previous node metric at node Dwhich is '0'
K_{SD} = shared symmetric key between S and D
K_{DB} = mutual key derived by nodes D and B
NMF_Sign = Signature of the NMFs of D

The PREPs unicasted by nodes *C* and *B* along the reverse paths to the source are as follows:

C→B :[K_C(prep || NMF_Sign ||h'$_c$ || $d_{h'c}$ || hc_C || m_C || pnm_C || d_1 || M_{CA})]

M_{CA} = h(({h'$_c$ || $d_{h'c}$}, hc_C, m_C, pnm_C, d_2), K_{CA})
d_2 = h(d_1)

B→A :[K_B(prep || NMF_Sign || h'$_c$ || $d_{h'c}$ || hc_B || m_B || pnm_B || d_2 || M_{BS})]

M_{BS} = h(({h'$_c$ || $d_{h'c}$}, hc_B, m_B, pnm_B, d_3), K_{BS})
d_3 = h(d_2)

It can be observed that the PREP frames are efficiently authenticated in route to the source node that generated the PREQ. These PREP frames are encrypted in transit with the one-hop group secret shared by the one-hop neighbors of a node and authenticated using HMAC to ensure two-hop authentication.

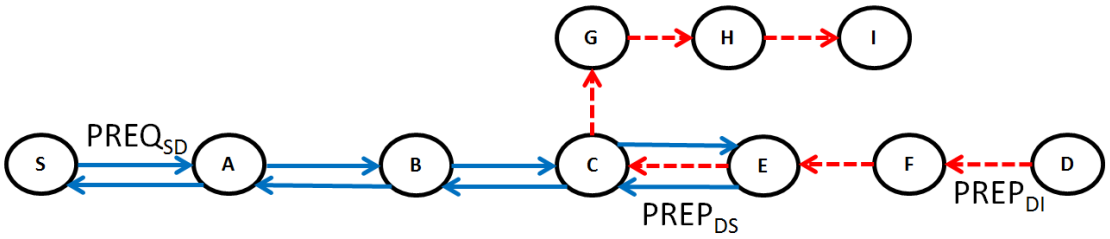

Fig. 4. Intermediate node reply (DO flag is not set)

In case an intermediate node already has a route to the destination due to its previous encounter with either a PREQ or PREP from the destination, it can generate a PREP to be unicasted to the source if the Destination Only (DO) flag is not set in the PREQ frame and if the last known sequence number of the destination in the PREQ that it just received is lower than the sequence number of the destination that the intermediate possesses in its route cache. In the example scenario discussed above where source node *S* is trying to find a route to destination node *D*, if node *C* already has a route to the destination node *D* and if DO flag in the PREQ from *S* is not set, *C* can generate a PREP. Refer to **Fig. 4**.

Source node *S* sends a $PREQ_{SD}$ in an attempt to find a route to the destination node *D*. In this scenario, node *C* already knows the route to *D* through a $PREP_{DI}$ that the node *D* has generated in response to a $PREQ_{ID}$ from node *I* in an attempt to find a route to node *D*. Node *C* will send a unicast PREQ to node *E*. Then, node *E* will see whether the intermediate node's special flag is set. This special flag will invoke node *E* to search in its cache a route to node *D* through its previous encounters of PREQ/PREP involving node *D*. In this scenario, node *E* will then send a special PREP to node *C* with its hop count, metric, previous node metric and other information, as shown below, from the $PREP_{DI}$ that it has in its cache sent from node *D* to node *I*.

$C \rightarrow E:[K_C(preq \parallel NMF\_Sign \parallel h_c \parallel s_{hc} \parallel hc_C \parallel m_C \parallel pnm_C \parallel s_3 \parallel M_2 \parallel B \parallel M_3 \parallel iFlag)]$

$M_3 = h((\{h_c \parallel s_{hc}\}, hc_C, m_C, pnm_C, s_4), T_C)$
$s_4 = h(s_3)$
$pnm_C = m_B$
iFlag = intermediate node flag set by node *C*. This flag will let node *E* know that *C* is sending this particular PREQ to authenticate the intermediate nodes on the way back to source node *S*. The reserved flag in PREQ frame format can be used for this purpose.

Node *E* will receive this PREQ as any other path request and process it to verify the authenticity. It will also observe the special intermediate flag (iFlag) is set and therefore, prepares a suitable PREP as follows:

$E \rightarrow C : [K_E(prep_E \| h'_c \| d_{h'c} \| hc_E \| m_E \| pnm_E \| d_2 \| M_{EB})]$

$M_{EB} = h((prep_E, \{h'_c \| d_{h'c}\}, hc_E, m_E, pnm_E, d_3), K_{EB})$
$d_3 = h(d_2)$
$prep_E - S \| D \| seq_D \| seq_S \| pr_D$
pr_D - PREQ or PREP that node *E* has encountered earlier and stored in its cache

Node *C* will receive the PREP from node *E* and will forward it to node *B* as in regular PREP propagation process, as shown in the figure. Node *B* will be able to verify if node *C* has modified the contents of the PREP from node *E* or not because *B* now has two-hop authentication from node *E*. Ideally, this process of intermediate node replying to a PREQ is an extension to the regular PREP reply process except that in this case the intermediate nodes fetches an extra step for authentication and verification purposes.

$C \rightarrow B : [K_C(prep_E \| h'_c \| d_{h'c} \| hc_C \| m_C \| pnm_C \| d_3 \| M_{CA})]$

$M_{CA} = h((prep_E, \{h'_c \| d_{h'c}\}, hc_C, m_C, pnm_C, d_4), K_{CA})$
$d_4 = h(d_3)$

4.5 Route Maintenance

4.5.1 Path Error (PERR)

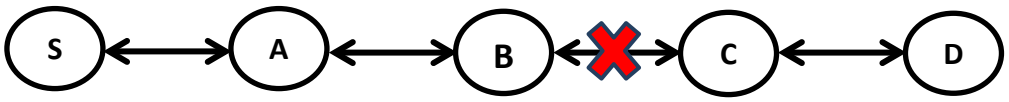

Fig. 5. PERR flow

Refer to **Fig. 5**. In the scenario, node B finds a broken link to node *C*. It will generate a PERR to its precursor mesh station, which in this case is node *A*, informing of the unreachability to node *C* through *B*. The following is the message extension field that is attached by node *B* to its PERR frame before sending it to node *A*. In this case, the NMFs of the PERR element and reason code [16] are signed using offline-online signature scheme. The only MF in PERR frame is element TTL and it is protected by encrypting the message extension field with a mutually shared key generated by a non-interactive key agreement scheme.

$B \rightarrow A : [K_{AB\text{-}PMK}(per \| NMF\_Sign \| TTL)]$

TTL = element TTL
$K_{AB\text{-}PMK}$ = pairwise master key (PMK) generated by SAE
NMF_Sign = Signature of the NMFs of 'PERR'
perr = NMFs || Reason Code

4.5.2 Gate Announcement (GANN)

When a mesh station is generating and sending a gate announcement frame announcing itself as the mesh gate, the gate announcement gets propagated in the network similar to PREQ. Therefore, the frame flow of GANN and RANN is similar to PREQ except that there is no set destination in GANN/RANN because it is an announcement to all the mesh stations. Refer to **Fig. 2**. In the following scenario, consider a mesh gate *S* generates a GANN frame to be propagated to the network of mesh stations. The following message extension field is attached by the mesh gate to its GANN/RANN to ensure the integrity of the frame. *S* randomly selects an initial hash value *hash* and hashes it h_c times to get $s_{hc} = h^h{}_c(hash)$. The NMFs of the GANN generated by the source node are signed using online/offline ID based signature scheme and are embedded in the GANN as shown below. Since NMFs do not change at every hop, intermediate node authentication is not necessary and therefore, the source node signs the NMFs of the HWMP GANN frame such as gate address, sequence number, lifetime, flags, Element ID, and Length. This signature is then embedded in the HWMP message extension for GANN and broadcasted.

$S \rightarrow *:[K_s(gann \| NMF\_Sign \| h_c \| s_{hc} \| hc_S \| s_0 \| M_0 \| B_S)]$

gann = Element ID || Length || Flags || Hop Count || Element TTL || gate mesh address || GANN Sequence Number || Interval
NMF_Sign = Signature of the NMFs of *S*
h_c = element TTL (maximum hop count)
s_{hc} = random value 'hash' hashed h_c times
hc_S = hop count at node *S*
T_S = secret chosen by *S* that is explicitly protected from all one-hop neighbors of *S*
$s_0 = h((h_c \| s_{hc}))$
$s_1 = h(s_0)$
$M_0 = h((\{h_c \| s_{hc}\}, hc_S, s_1), T_S)$
Bs = broadcast secret of *S*

The one-hop neighbors of *S* will be able to decrypt the GANN using the key K_S that was shared by *S* earlier. A neighbor node *A* will decrypt the GANN broadcasted by *S*, increment the hop count, decrement the element TTL, and broadcast it by encrypting using its one-hop secret key K_A that it had shared with its one-hop neighbors as well. Note that it does not have access to *S*'s broadcast secret T_S.

$A \rightarrow *:[K_A(preq \| NMF\_Sign \| h_c \| s_{hc} \| hc_A \| s_1 \| M_0 \| S \| M_1)]$

$M_1 = h((\{h_c \| s_{hc}\}, hc_A, s_2), T_A)$
$s_2 = h(s_1)$

Propagation of the GANN frame to nodes *B*, *C* and *D* proceeds in a similar fashion.

4.5.3 Root Announcement (RANN)

The message flow of RANN is very similar to that of a GANN except that the MFs of RANN in the message extension field include metric and previous node metric. For a scenario similar discussed in GANN, the message extension field will be as follows:

$S \rightarrow *:[K_s(\text{rann} \| \text{NMF\_Sign} \| h_c \| s_{hc} \| hc_S \| m_S \| pnm_S \| s_0 \| M_0 \| B_S)]$

rann = Element ID || Length || Flags || Hop Count || Element TTL || root mesh address || HWMP Sequence Number || Interval || Metric
NMF_Sign = Signature of the NMFs of *S*
h_c = maximum hop count
s_{hc} = random value 'hash' hashed h_c times
hc_S = hop count at node *S*
m_S = airtime metric at node *S*
pnm_S = previous node metric at node *S* (0 for source node)
T_S = secret chosen by S that is explicitly protected from all one-hop neighbors of *S*
$s_0 = h((h_c \| s_{hc}))$
$s_1 = h(s_0)$
$M_0 = h((\{h_c \| s_{hc}\}, hc_S, m_S, pnm_S, s_1), T_S)$

5. Security Analysis

In this section, the security analysis of the proposed scheme is presented. The robustness of the proposed scheme against various known attacks is evaluated.

Path diversion attack: An attacker can create a blackhole/wormhole by launching a path diversion attack in a WMN. The attacker can lower the airtime metric in the HWMP frames to smaller values when compared to other paths thereby, diverting the route taken by the frame to another route as desired by the attacker. Also, the attacker can increase the sequence number on such a frame to trick the victims to believe that this is the most recent frame. The ID based online/offline signature scheme helps the detection of the illegal modification of the sequence number by an intermediate node. Two-hop authentication provided by the broadcast encryption technique will detect any fake metric changes by intermediate nodes. If an attacker decides to alter the metric, the neighboring node would detect the alteration because of the two-hop authentication that it verifies from the node previous to the attacker.

Impersonation attack: An attacker can gain access to the contents of HWMP frames by using an impersonation attack. This can be accomplished by the attacker pretending as a root mesh station and sending out announcements to gather replies from the mesh stations. The ID based offline/online signature scheme used in the proposed scheme requires every mesh node to sign the PREQ/RANN frame before sending out. Therefore, the attacker will not be able to launch an impersonation attack because the attacker will not be able to spoof itself to somebody else as it does not have access to the secret user key, computed and pre-distributed to every mesh node by a private key generator, for generating the appropriate digital signature.

Flooding attack: An external attacker might be able to flood the network by continuously broadcasting frames with false information. This is a type of denial of service attack and can heavily impact the performance of a network. In order to avoid such attacks, the proposed scheme uses one-hop and two-hop authentication alongside digital signature scheme so that any non-authenticated broadcasting message will be immediately dropped by any receiving mesh station in the network.

Passive attack: An attacker can perform a passive attack in which the main goal is to obtain the important information about the WMN. The proposed scheme has mesh stations with one-hop group secret keys, broadcast secrets for two-hop authentication which provide protection against passive attacks because the attacker cannot obtain the contents of the encrypted message without the knowledge of the appropriate keys.

Replay attack: To avoid replay attacks in the WMN, a timestamp concept used in [11] is applied in our proposed framework. This timestamp concept permits a receiving mesh node to validate the received signed messages based on the time interval within which it has received the frame. Consequently, a signed message, injected by a replay attacker, arriving with timestamp discrepancy will be dropped. The timestamp approach used here is based on the 802.11 MAC layer parameters and on mesh node capabilities in term of buffering and CPU processing. Moreover, this proposition of timestamp discrepancy enables mesh nodes to limit and reduce the redundant messages injected by a replay attacker.

6. Performance Evaluation

6.1 Simulation Environment

To investigate the performance of the proposed scheme, it is necessary to estimate the time overhead involved on the processing of the frame. The HWMP routing frames such as PREQ, PREP, PERR, RANN and GANN are encrypted and certainly, there will be overhead involved in encryption and decryption that should be taken into consideration in the simulations. The simulations were run on a workstation with Intel® 2.00 GHz CPU and 4 GB of RAM running Ubuntu 12.04 Linux OS with ns-3 installed. Both MIRACL library [14] and RELIC Toolkit [15] are integrated and compiled with ns-3 and therefore, all the simulation results already include the delay incurred by the cryptographic primitives used in the proposed scheme.

Our proposed security framework for HWMP was implemented in *ns-3* simulator and the performance of the protocol was evaluated by comparing it with the standard version of the HWMP and SHWMP [6]. *ns-3* seems appropriate simulation tool because of its support for 802.11s standard as well as HWMP. The network in the simulation scenario consists of varying number of mesh devices setup in square grid topology. In order to integrate the online/offline signature scheme and non-interactive key agreement scheme in HWMP, MIRACL library and RELIC Toolkit library are utilized.

MIRACL is available as an open source software development kit (SDK) for ECC over GF(p). This is convenient to use C and C++ library for large integers and rational numbers

which has all the implementations of the necessary primitives for the implementation of the cryptographic code. It also fully supports ECC over GF(p) and GF(2^m) which is required for the ID based signature generation and verification stages of the online/offline signature scheme in the proposed approach. For the proposed scheme, the usage of at least 160-bit keys is recommended by NIST when using ECC. This will allow attaining a security level comparable with the standard RSA based implementations with a key size of 1024-bits. In the implementation of online-offline scheme, verifiably random elliptic curve domain parameters (shown in **Table 2**) over F_p are used which are generated by a point-counting algorithm available in the MIRACL library known as Schoof's algorithm that generates a completely random curve and directly counts the points on it.

Table 2. Elliptic curve domain parameters used

Key length	160 bits
p	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF7FFFFFFF
a	-3
b	44C1A1CE9
q	FFFFFFFFFFFFFFFFFFF609BC7611575926DB777
x	A2948EBFEE94136952AFEB4C87FD1B99E6DF632
y	52C9D3E6B2A3FC50FC0D0AD36656383088C31A78

In the proposed approach, non-interactive key agreement scheme is used for which Relic-Toolkit is a good choice because it has the implementation for Sakai-Ohgishi-Kasahara authenticated key agreement scheme **[5]** which is used for authentication between mesh stations during the path reply phase of the routing. In the implementation of this scheme in Relic Toolkit, a master secret key (MSK) is generated by a key management service (KMS) and then a public key is derived from the MSK. For each mesh station, a receiver secret key (RSK) is derived from the ID of the mesh station, the public key and the MSK. The public key with the corresponding RSK is distributed by the KMS to each of the mesh stations prior to the routing through authenticated channel. When each mesh station receives the key material, it verifies the authenticity of the information received. A mesh station will send encapsulated data that is formed using the KMS public key to another mesh station that it wants to communicate with. The other mesh station, upon receiving the data, processes it with the RSK and derives a shared secret that can be used to encrypt the messages between the two nodes under consideration.

Relic-Toolkit has functions that can be utilized to create MSK and RSK which are then used in the PREP phase for authentication between intermediate nodes. The required keys for this implementation generated by the KMS are assumed to have been pre-distributed among the mesh stations in the network using a suitable key distribution scheme. Since it is an ID based key agreement scheme, the MAC addresses of the mesh stations are used as the identifiers for generating the user private keys.

Table 3 lists simulation setup parameters used in this section.

Table 3. Simulation setup parameters

Parameter	Value	Parameter	Value
Area	600m x 600m	Number of nodes	9 - 36
Stack	802.11s	Total Duration	300 seconds
Packet Size	1024 bytes	Distance between nodes	170 m
Data rate	50 - 400 Kbps	Topology	Square Grid
Packet Interval	0.1 seconds	Traffic	User Datagram Protocol
Routing Protocol	HWMP		

To evaluate the performance of the proposed protocol, the standard HWMP, SHWMP [6] and the proposed protocol are subjected to run through the same simulation setup. The three major parameters of interest in this simulation are throughput, end-to-end delay, and packet delivery ratio. For varying number of nodes in the network and the distance between them, the aforementioned parameters are recorded from the simulation results and the performance of the proposed protocol was deduced from the obtained data. Following are the definitions of the parameters that are used for evaluation:

1) Throughput: Average rate of bits received over a period of time. It can be calculated by dividing the number of bits received by the difference between the arrival time of the first and last packets
2) End-to-end delay: Average time taken by a data packet to travel from the source node to the destination node. It can be calculated by dividing the sum of the time taken by each packet to reach the destination with the number of packets received by the destination.
3) Packet delivery ratio: It is the ratio of the number of packets received to the number of packets sent.

6.2 Simulation Result

Fig. 6, 7, 8 are the throughput, end-to-end delay and packet delivery ratio, respectively, measured against varying transmission rates in a 3 × 3, 4 × 4, 5 × 5 and 6 × 6 grid setup. From the figures, it can be observed that although our proposed version of HWMP protocol (SecHWMP) does suffer in terms of throughput, end-to-end delay and packet delivery ratio, it still performs significantly well even with multiple security mechanisms involved which are employed to protect both the mutable and non-mutable fields of the HWMP routing frames. It can be observed from the results that in the worst case scenario, when compared to the standard HWMP, the throughput of the proposed approach suffers only 29% decrease in a densely populated 5 × 5 grid. Similarly, end-to-end delay suffers a worst case 30% decrease in a 6 × 6 grid. The worst case packet delivery ratio from the simulation results is approximately 48%.

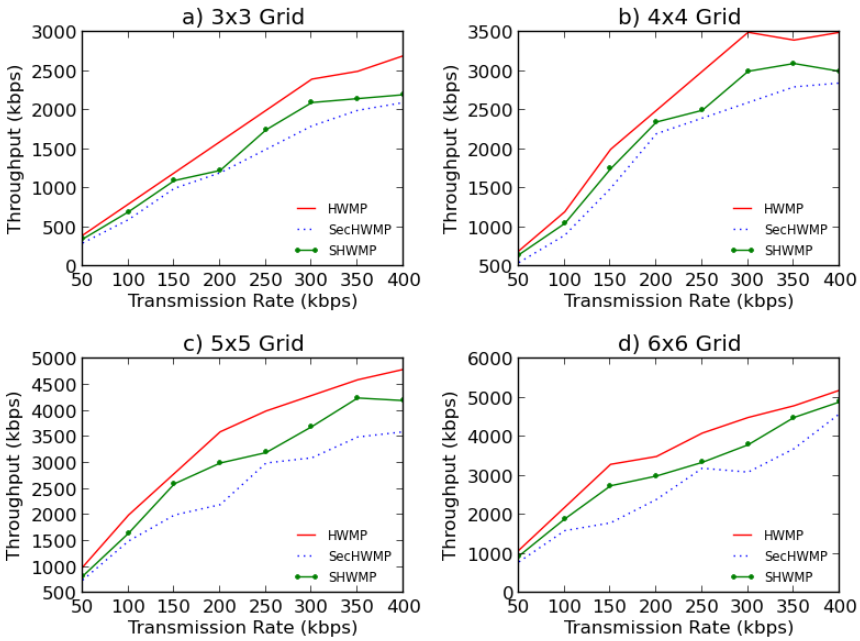

Fig. 6. Throughput vs. transmission rate

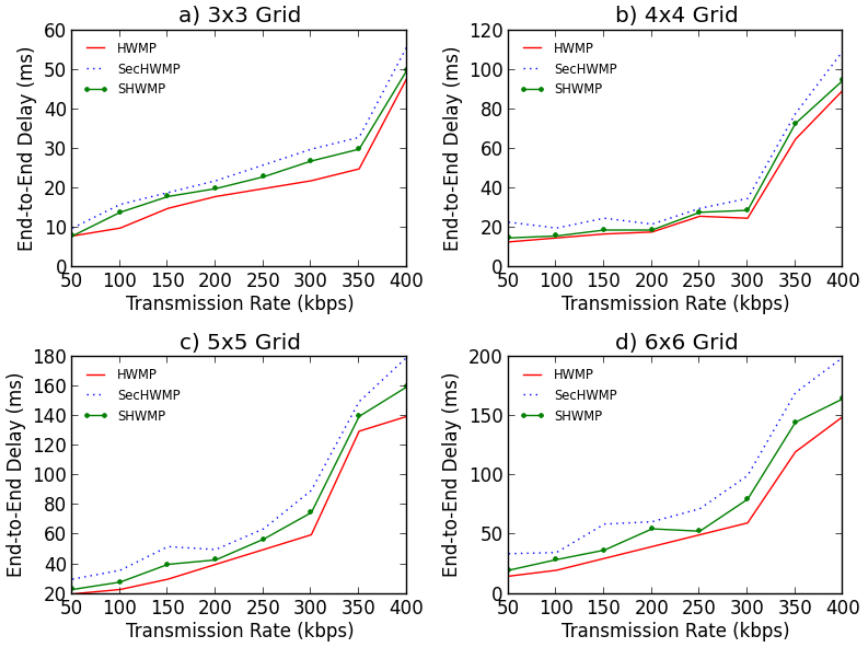

Fig. 7. End-to-End Delay vs. transmission rate

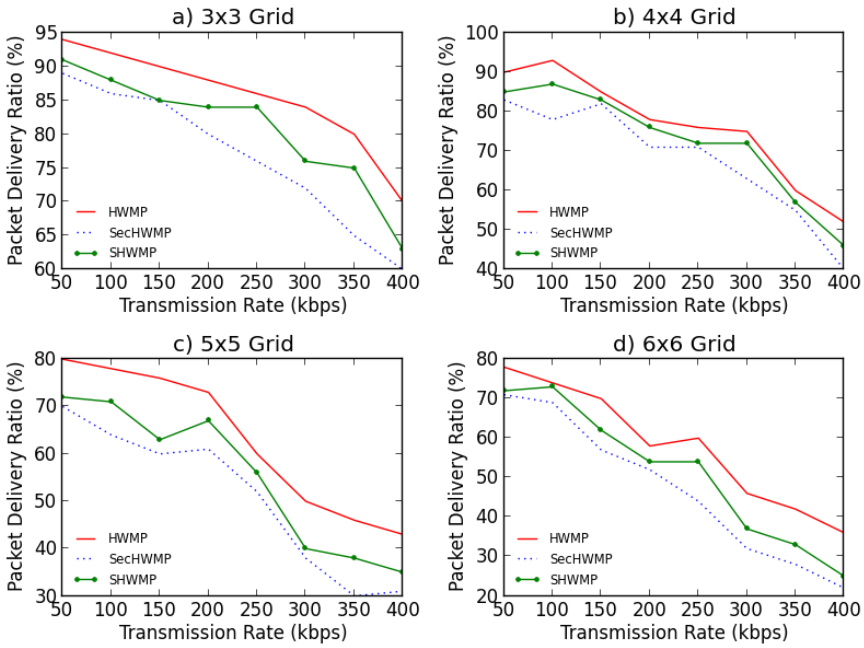

Fig. 8. Packet Delivery Ratio vs. transmission rate

The proposed scheme provides integrity assurance from the source node to the destination node to protect against NMF modification attacks, security features for PERR frames and robustness against internal attacks which are not provided by SHWMP. These features are incorporated at the sacrifice of slight performance degradation when compared to SHWMP and the standard HWMP, and the degradation is worthwhile considering the seriousness of the security concerns of WMNs.

7. Conclusion

In this paper, the security concerns of the Hybrid Wireless Mesh Protocol (HWMP), the default routing protocol of WMNs, are identified. Based on the evaluation of security requirements of WMNs, a security framework for HWMP is proposed. The proposed approach integrates two security schemes: offline/online signature scheme to provide end-to-end authentication to non-mutable fields of HWMP and non-interactive key agreement scheme coupled with broadcast encryption scheme to provide point-to-point security to mutable fields of HWMP. This is accomplished by embedding extra fields to the existing routing frames of HWMP which carry additional authentication information for the nodes to verify before processing or forwarding the frames. Finally, the performance of the proposed secure version of HWMP is evaluated by comparing with the traditional HWMP protocol through extensive simulations in ns-3 simulator. The simulation results suggest that the proposed approach has reasonable performance degradation due to the additional security mechanisms employed.

References

[1] Joseph K. Liu, Joonsang Baek, Jianying Zhou, Yanjiang Yang, and Jun Wen Wong, "Efficient online/offline identity-based signature for wireless sensor network," *Int. J. Inf. Secur*,. 9(4), pp. 287-296, August 2010. Article (CrossRef Link)

[2] M. Ramkumar, "Broadcast Encryption Using Probabilistic Key Distribution and Applications," *Journal of Computers*, June, 2006. Article (CrossRef Link)

[3] Sivakumar, K.A.; Ramkumar, M., "Safeguarding Mutable Fields in AODV Route Discovery Process," In *Proc. of Proceedings of 16th International Conference on Computer Communications and Networks*, ICCCN 2007, pp. 645-651, 13-16 Aug. 2007. Article (CrossRef Link)

[4] Oliveira, L.B.; Scott, M.; Lopez, J.; Dahab, R., "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," In *Proc. of 5th International Conference on Networked Sensing Systems, INSS 2008*, pp.173-180, 17-19 June, 2008. Article (CrossRef Link)

[5] R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing. In *2000 Symposium on Cryptography and Information Security (SCIS2000)*, 2000. Article (CrossRef Link)

[6] Islam. M.S; Hamid, M.A.; Hong. C.S., "SHWMP: A Secure Hybrid Wireless Mesh Protocol for IEEE 802.11s Wireless Mesh Network," *Transaction on Computational Science* 2009, 6, 95-114. Article (CrossRef Link)

[7] A. Egners: *Evaluating IEEE 802.11s Against Security Requirements of Wireless Mesh Networks*, Essener Workshop zurNetzsicherheit 2010 (EWNS10), April 2010. Article (CrossRef Link)

[8] S. D. Galbraith, "Pairings," in Advances in Elliptic Curve Cryptography, ser. London Mathematical Society Lecture Notes, I. F. Blake, G. Seroussi, and N. Smart, Eds. Cambridge Univ. Press, 2005, vol. 317, ch. IX, pp. 183–213. Article (CrossRef Link)

[9] Eike Kiltz and Gregory Neven. In M. Joye and G. Neven, editors, *Identity-based cryptography*, volume 2 of *Cryptology and Information Security Series*, pages 31-44. IOS Press, 2008. Article (CrossRef Link)

[10] Athina Lazakidou, Konstantinos Siassiakos and Konstantinos Ioannou, "Wireless Technologies for Ambient Assisted Living and Healthcare," *1st ed. Hershey*, PA: IGI, 2010. Article (CrossRef Link)

[11] A. Baayer, N. Enneya and M. Elkoutbi, "Enhanced Timestamp Discrepancy to Limit Impact of Replay Attacks in MANETs," *Journal of Information Security*, Vol. 3, No. 3, pp. 224-230, 2012. Article (CrossRef Link)

[12] Ramkumar, Mahalingam, and Nasir Memon, "An efficient key predistribution scheme for ad hoc network security," *Selected Areas in Communications*, IEEE Journal on 23.3 (2005): 611-621, 2005. Article (CrossRef Link)

[13] Jerome Henry, "802.11s Mesh Networking," *cwnp*. 2011. 15 August 2013. Article (CrossRef Link)

[14] Scott M., *MIRACL-A Multiprecision Integer and Rational Arithmetic C/C++ Library*, Shamus Software Ltd, Dublin, Ireland, 2003. Article (CrossRef Link)

[15] D.F. Aranha and C. P. L. Gouv, *RELIC is an Efficient LIbrary for Cryptography*, 2009. Article (CrossRef Link)

[16] IEEE Standard for Information Technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking," IEEE Std 802.11s-2011 (Amendment to IEEE Std 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, IEEE 802.11w-2009, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11z-2010, IEEE 802.11v-2011, and IEEE 802.11u-2011), pp. 1,372, Sept. 10 2011. Article (CrossRef Link)

[17] Charles E. Perkins, Elizabeth M. Belding Royer, Samir R. Das: Adhoc On-Demand Distance Vector (AODV) Routing. RFC 3561, November 2003. Article (CrossRef Link)

[18] Ben-Othman, J., Benitez, Y.I.S., "IBC-HWMP: A novel secure identity-based cryptography-based scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11s," *Concurrency and Computation: Practice and Experience* 2011. Article (CrossRef Link)
[19] Tan, W.K., Lee, S.-G., Lam, J.H., Yoo, S.-M. "A Security Analysis of the 802.11s Wireless Mesh Network Routing Protocol and Its Secure Routing Protocols," *Sensors 2013*, 13, 11553-11585, 2013. Article (CrossRef Link)
[20] Ben-othman, J., Benitez, Y.I.S., "A light weight security scheme for HWMP protocol using Elliptic Curve technique," in *Proc. of Proceeding of the 11th IEEE International Workshop on Wireless Local Networks (WLN'11)*, pp. 850-854, Bonn, Germany, 4-7 Oct. 2011. Article (CrossRef Link)
[21] A. Jivsov, "Compact representation of an elliptic curve point," *IETF. draft-jivsov-ecc-compact-02*, June 2013. Article (CrossRef Link)
[22] Ben-Othman, J. Claude, J. Benitez, Y.I.S., "A novel mechanism to secure internal attacks in HWMP routing protocol," in *Proc. of Proceeding of IEEE International Conference on of Communications (ICC) 2012*, pp. 162-166, Ottawa, Canada, 10-15 June 2012. Article (CrossRef Link)
[23] Y.-C. Hu, A. Perrig, and D. Johnson. Ariadne, "A secure on-demand routing protocol for ad hoc networks," in *Proc. of Proceedings of the ACM Conference on Mobile Computing and Networking (Mobicom)*, 2002. Article (CrossRef Link)

Mallikarjun Avula is a Ph.D. candidate in Computer Engineering from Electrical and Computer Engineering Department, UAHuntsville. He received Master of Science degree in Electrical Engineering from University of Alabama in Huntsville (UAHuntsville) in December 2009 and Bachelor of Technology degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University, India in May 2007. His primary research interests are wireless mesh networks, wireless sensor networks, and network security.

Sang-Gon Lee received his BEng, MEng, and PhD degrees in electronics engineering from Kyungpook National University, Rep of Korea, in 1986, 1988, and 1993, respectively. He is a professor in the Division of Computer & Information Engineering, Dongseo University. He was a visiting scholar at QUT, Australia, from August 2003 to July 2004 and at the University of Alabama at Huntsville, USA, from July 2012 to Jun 2013. His research areas include information security, network security, wireless mesh/sensor networks, and the future Internet.

Seong-Moo Yoo is an Associate Professor of Electrical and Computer Engineering at the University of Alabama in Huntsville (UAH). Before joining UAH, he was an Assistant Professor at Columbus State University, Columbus, Georgia –USA. He earned MS and PhD degrees in Computer Science at the University of Texas at Arlington. His research interests include computer network security, wireless network routing, and parallel computer architecture. He has co-authored over 90 scientific articles in refereed journals and international conferences. He is a senior member of IEEE and a member of ACM.