Securing Layer-2 Path Selection in Wireless Mesh Networks

Md. Shariful Islam[1], Md. Abdul Hamid[1], Byung Goo Choi[1] and Choong Seon Hong[1]

[1] Department of Computer Engineering, Kyung Hee University, Republic of Korea.
{sharif,hamid}@networking.khu.ac.kr,
{bgchoi,cshong}@khu.ac.kr

Abstract. The current draft standard of 802.11s has defined routing for Wireless Mesh Networks (WMNs) in layer-2 and to differentiate from layer-3 routing, it termed layer-2 routing as path selection. The layer-2 path selection (LPS) mechanism is fully specified in the draft of IEEE 802.11s for WMNs. However, routing with security provision is not specified in the standard. Our study identifies that the current path selection mechanism is vulnerable to various types of routing attacks like flooding, route re-direction, spoofing etc. In this paper, we develop a novel Secure Layer-2 Path Selection (SLPS) mechanism that uses cryptographic extensions to provide authenticity and integrity of routing messages. Particularly, the proposed SLPS prevents unauthorized manipulation of mutable fields in the routing messages. Results from analysis and simulation demonstrate that SLPS protocol is robust against identified attacks and provides higher packet delivery ratio, requires no extra communication cost and incurs little path acquisition delay, computational and storage overhead to accomplish secure path selection.

Keywords: Security, Merkle Tree-based Authentication, Layer-2 Routing, Wireless Mesh Networks.

1 Introduction

The area of wireless networks has gained increased importance and development during the past decade. Wireless Mesh Networks (WMN) have emerged as a key technology to support a numerous number of application scenarios like broadband home networking, community and neighborhood networking, enterprise networking, metropolitan area networking, etc. It is a paradigm shift from conventional 802.11 WLAN for its unique

"This research was supported by the MKE under the ITRC support program supervised by the IITA" (IITA-2008-(C1090-0801-0016)). Dr. C. S. Hong is the corresponding author.

characteristics of self-configuring capability, easy network maintenance, lower cost and robustness [1]. Wireless mesh architecture's infrastructure is, in effect, a router network minus the cabling between nodes. It is built of peer radio devices that do not have to be cabled to a wired port like traditional WLAN access points (AP) do and such architecture provides high bandwidth, spectral efficiency, and economic advantage over the coverage area. As a result, the increased interest in WMN has demanded a standard named IEEE 802.11s. The current draft D1.06 [2] of 802.11s is the first to introduce the concept of embedding routing in layer-2. The main motivation that drives incorporating routing in MAC layer is the interoperability between devices of different vendors.

The network architecture of a 802.11s WMN is depicted in Fig. 1. A mesh point (MP) is an IEEE 802.11s entity that can support WLAN mesh services. A mesh access point (MAP) is an MP but can also work as an access point. A mesh portal (MPP) is a logical point that connects the mesh network to other networks such as a traditional 802.11 WLAN or a non-802.11 network. The current 802.11s standard defines secure links between MPs, but it does not provide end-to-end security [3]. Also, the security in routing or forwarding functionality is not specified in 802.11s standard. Routing information elements are transferred in plain text and are prone to various types of routing attacks like flooding, route re-direction, spoofing, etc. The main reason is that intermediate nodes need to modify mutable fields (i.e., hop count, TTL, metric, etc.) in the routing element before forwarding and re-broadcasting them. Since other nodes will act upon those added information, these must also be protected somehow from being forged or modified. However, only source authentication does not solve this problem, because the information is added or modified in intermediate nodes. This motivates us to include hop-by-hop authentication in our proposal. More specifically, each node that adds information in the control packet should authenticate the added information in such a way that each other node acts upon that information should be able to verify its authenticity.

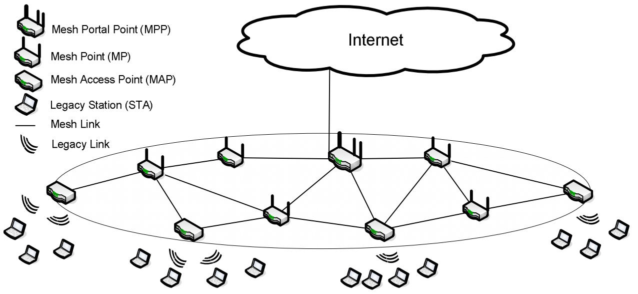


Fig. 1. Network architecture: Wireless Mesh Networks.

We develop a Secure Layer-2 Path Selection (SLPS) protocol for wireless mesh networks. SLPS takes into consideration the existing key hierarchy of 802.11s, identifies the mutable and non-mutable fields in the routing message, protects the non-mutable part using symmetric encryption and authenticates mutable information using Merkle tree [4].

Particularly, the proposed SLPS prevents unauthorized manipulation of mutable fields in the routing messages. Results from analysis and simulation demonstrate that SLPS protocol is robust against the identified attacks, provides higher packet delivery ratio, requires no extra communication cost and incurs little computational and storage overhead. Table 1 depicts the notations and abbreviations used throughout the paper.

Table 1. Notations and abbreviations used in this paper.

Notation	Meaning
PREQ	Path request message
PREP	Path reply message
PREQ/PREP-MF	Path request or reply message excluding the mutable fields
RANN	Root announcement message
GTK	Group transient key
PTK	Pairwise transient key
MAC	Message authentication code
$MAC_k root(x)$	MAC created on the root of the Merkle Tree using key *k* by the node *x*
h(v)	A hash created on the mutable field *v*
||	Concatenation of messages
authpath(v)	Authentication path for the mutable field *v*

The rest of the paper is organized as follows. Section 2 discusses related works. Section 3 briefly introduces existing L-2 path selection (LPS) mechanism in 802.11s. Security vulnerabilities of existing path selection mechanism are identified in Section 4. We describe our proposed secure routing (SLPS) in Section 5. Security analysis and performance evaluation are carried out in Section 6 and 7, respectively. Finally, we conclude the paper in Section 8.

2 Related Works

Security is a critical step to deploy and manage WMNs. Since the access to any deployed wireless mesh network is possible for any wireless enabled device, it should be ensured that only authorized users are granted networks' access. As of now, there is no state-of-the-art solution exists in the literature for securing L2 routing in 802.11s. In [5], the authors have just summarized the proposed routing from 802.11s draft. Ref [6] describes just an update of layer-2 routing in the current draft. A framework for 802.11s and research challenges are summarized in [3]. A hybrid centralized routing protocol is presented in [13] that incorporates tree-based routing with a root-driven routing protocol. Apart from these, there has been some research on securing layer 3 routing. Ariande in [7] ensures a secure on-demand source routing. Authentication is done using TESLA [8], digital signatures and standard MAC. However, as the route request is not authenticated until it reaches the destination, an adversary can initiate route request flooding attack. A variant of Ariande [7] named endairA is proposed in [9] with the exception that instead of signing a route request, intermediate nodes sign the route reply. However, endairA is still vulnerable to malicious route request flooding attack. SAODV [10] is a secure variant of AODV in which operations are similar to AODV, but uses cryptographic extensions to provide authenticity and integrity of routing message. It uses hash chains in order to prevent manipulation of hop count field. However, an adversary may always increase the hop count. Another secure on-demand distant vector protocol, ARAN (Authenticated Routing for Ad hoc Networks), is presented in [11]. Just like SAODV, ARAN uses public key cryptography to ensure integrity of routing message. However, a major drawback of ARAN is that it requires extensive signature generation and verification during the route request flooding which may result in denial-of-service attack.

Our secure path selection scheme employs only symmetric cryptographic primitives and does not assume the existence of pairwise shared key for source-destination. Rather, a Merkle tree-based hop-by-hop authentication mechanism is devised exploiting existing keying hierarchy of 802.11s standard.

3 Path Selection Mechanism in 802.11s

The layer-2 path selection (LPS) mechanism defined in 802.11s is a combination of both reactive and proactive strategy by employing both on-demand path selection mode and proactive tree building mode [2] [5] [6]. The mandatory routing metric used is the airtime cost metric [2] that measures the amount of channel resource consumed by transmitting a frame over a particular link. In LPS mechanism, both on demand and proactive mode can be used simultaneously. In the On-demand mode, a source MP broadcasts *path request* (PREQ) message requesting a route to the destination. The PREQ is processed and forwarded by all intermediate MPs and set up the reverse path from the destination to the source of route discovery. The destination MP or any intermediate MP with a path to the destination may unicast a *path reply* (PREP) to the source MP that creates the forward path to the destination.

Proactive Tree Building mode builds a tree-topology network when a root in the WMN is configured. This topology tree formation begins when the root starts to periodically broadcast a root announcement (RANN) message which propagates the metric information across the network. Upon reception of a RANN message, an MP that wants to create or refresh a path to the root MP sends a unicast PREQ to the root MP. The root MP then unicasts a PREP in response to each PREQ. The unicast PREQ creates the reverse path from the root MP to the originating MP, while the PREP creates the forward path from the MP to the root MP. A root MP may also proactively disseminate a PREQ message to all the MPs in the networks with the intention to establish a path. An MP, after receiving a proactive PREQ, creates or updates its path to the root MP by unicasting a *Proactive* PREP.

Path selection mechanism also allows both on-demand and proactive mode to work simultaneously. This hybrid mode is used in situations where a root MP is configured and a mesh point S wants to send data to another mesh point D but has no path to D in its routing table. Instead of initiating on demand mode, S may send data to the root MP, which in turns delivers the data to D informing that both S and D are in the same mesh. This will trigger an on-demand route discovery between S and D and subsequent data will be forwarded using the new path.

4 Possible Attacks

In this section, we show that LPS, in its normal operation, is vulnerable to the following attacks.

4.1 Flooding Attack

It is very easy for a malicious node to flood the network with a PREQ messages destined to an address which is not present in the network. As the destination node is not present in the network, every intermediate node will keep forwarding the PREQ messages. As a result, a large number of PREQ messages in a short period will consume the network bandwidth and can degrade the overall throughput.

4.2 Route Re-direction Attack

A malicious node M may divert traffic to itself by advertising a route to a destination with a destination sequence number (DSN) greater than the one it received from the destination. For example, the malicious node M in Fig. 2a receives a PREQ from A which was originated from S for a route to node D. As LPS allows intermediate PREP, M may unicast a PREP to A with a higher DSN than the value last advertised by D. So, A will re-direct all subsequent traffic destined for D to the malicious node M.

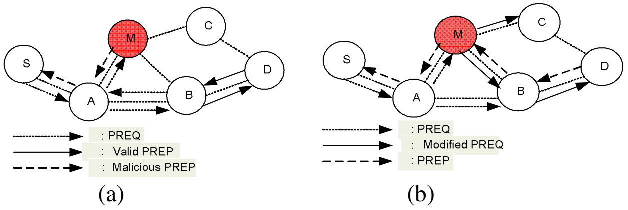


Fig. 2. Route re-direction attack. (a) Increasing DSN. (b) Decreasing metric.

Route re-direction attack can also be launched by modifying the mutable metric field used in the LPS PREQ messages. A malicious node can modify the mutable metric field to zero to announce a better path to a destination. As depicted in Fig. 2b, M can decrease the metric field in the PREQ to zero and re-broadcasts it to the network. So, the reverse path created should go through the malicious node M. As a result, all traffics to the destination D will be passed through the attacker.

4.3 Routing Loops

A malicious node may create routing loops [11] in a mesh network by spoofing MAC addresses and modifying the value of the metric field. Consider the following network scenarios (Fig. 3) where a path exists between the source S and destination X that goes through node B and C. Also, there exists a path from A to C through D.

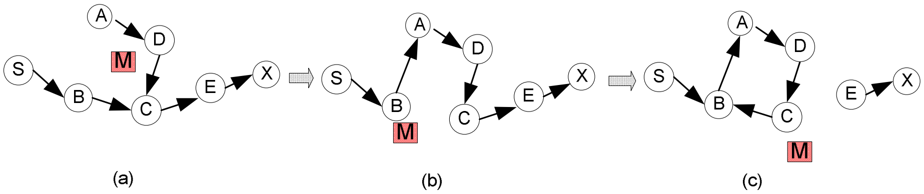


Fig. 3. Routing loops formation**.**

Assume that a malicious node M, as shown in Fig. 3a, is present in the vicinity where it can listen to the PREQ/PREP messages that pass through A, B, C and D during route discovery process. It may create a routing loop among the nodes A, B, C and D by impersonation combined with modification of metric field in PREP message. First, it impersonates node A's MAC address and moved out of the reach of node A and closer to node B. And then it sends a PREP message to node B indicating a better metric value then that of the value received from C. So, node B now re-establishes its route to X that should go through A as shown in Fig 3b. At this point, the malicious node impersonates node B and moves closer to node C and sends a PREP to node C indicating a better metric then the one received from E. So, node C will now choose B as the next hop for its route to the destination X as shown in Fig 3c. Thus a loop has been formed and the destination X is unreachable from all the four nodes.

5 Proposed Secure Layer-2 Path Selection (SLPS) Protocol

SLPS, proposed in this section is a secure extension of LPS. As specified in [2], LPS routing information elements have a mutable and a non-mutable part. We exploit these existing mutable and non-mutable fields to design a secure layer-2 path selection. Particularly, SLPS mechanism has four components: (1) key establishment, (2) identifying the mutable and non-mutable fields, (3) showing that the mutable fields can be authenticated in a hop-by-hop fashion using the concept of Merkle tree, and finally (4) protection of non-mutable fields is achieved with the use of symmetric encryption. We present our approach in details in the following subsections.

5.1 Key Establishment

Entities in a WMN can act both as supplicant MP or mesh authenticator (MA). Before initiating a route discovery process, all the MPs authenticate its neighboring MPs, establish pairwise transient key (PTK), and send the group transient key (GTK) through key distribution and authentication process of 802.11s as depicted in Fig 4. We use this GTK for securing broadcast messages (e.g., PREQ, RANN) and PTK for securing unicast messages (e.g., PREP, proactive PREQ).

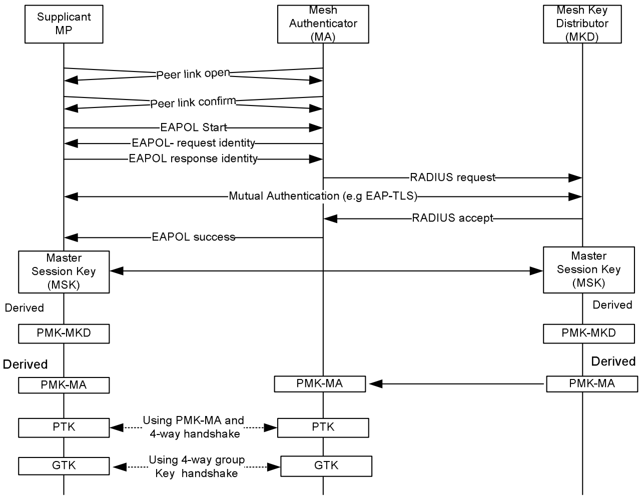


Fig. 4. Key distribution and authentication in 802.11s.

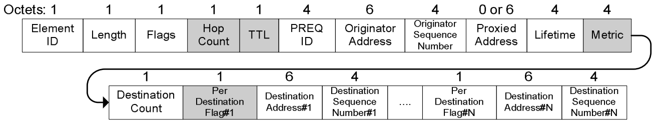
5.2 Identifying Mutable and Non-mutable Fields

The information elements in the LPS contain mutable fields that are modified in the intermediate routers and non-mutable fields that are not modified in the intermediate routers. The identified mutable fields in the PREQ (Fig. 5) element are:

Hop count field: Provides information on the number of links in the path, incremented by each intermediate node, but it is not used for routing decision.

TTL field: The time-to-live field defines the scope of the PREQ in number of hops. TTL value is decremented by 1 at each intermediate node.

Metric field: Unlike AODV, LPS uses an airtime link metric instead of hop count metric to take a decision on path selection. Whenever an intermediate node receives a PREQ that is to be forwarded, it calculates the airtime cost in the current path and adds the value to the existing metric field.

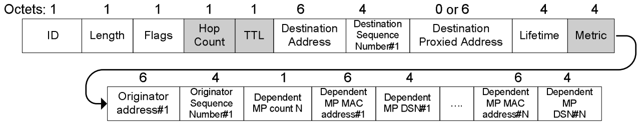


Octets: 1	1	1	1	1	4	6	4	0 or 6	4	4
Element ID	Length	Flags	Hop Count	TTL	PREQ ID	Originator Address	Originator Sequence Number	Proxied Address	Lifetime	Metric

1	1	6	4		1	6	4
Destination Count	Per Destination Flag#1	Destination Address#1	Destination Sequence Number#1	….	Per Destination Flag#N	Destination Address#N	Destination Sequence Number#N

Fig. 5. PREQ message format.

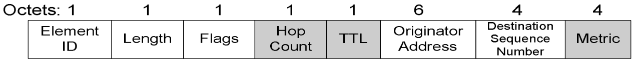
Per destination flag: The Destination Only (DO) and Reply and Forward (RF) Flag determine whether the route-reply message (RREP) will be sent by intermediate node or only by the destination. If DO flag is not set and RF flag is set, the first intermediate node that has a path to the destination sends PREP and forwards the PREQ by setting the DO flag to avoid all intermediate MPs sending a PREP. In this case, per destination flag field is also a mutable field. Fig. 6 and Fig. 7 show the format of a PREP and RANN information element. In both the cases, the mutable fields are hop-count, TTL and metric indicated by the shadowed boxes.



Octets: 1	1	1	1	1	6	4	0 or 6	4	4
ID	Length	Flags	Hop Count	TTL	Destination Address	Destination Sequence Number#1	Destination Proxied Address	Lifetime	Metric

6	4	1	6	4		6	4
Originator address#1	Originator Sequence Number#1	Dependent MP count N	Dependent MP MAC address#1	Dependent MP DSN#1	….	Dependent MP MAC address#N	Dependent MP DSN#N

Fig. 6. PREP message format.



Octets: 1	1	1	1	1	6	4	4
Element ID	Length	Flags	Hop Count	TTL	Originator Address	Destination Sequence Number	Metric

Fig. 7. RANN message format.

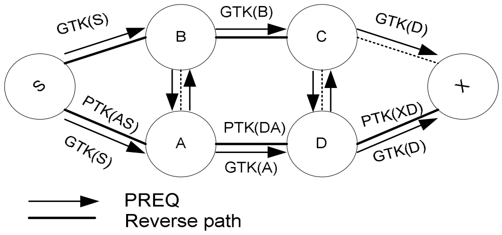


Fig. 8. Secure on-demand path selection.

5.3 Secure Route Discovery

1) Securing On demand mode: This mode is used when there is no root MP configured or a root MP is configured, but on demand mode can provide a better path to another MP. Consider a source MP *S* in Fig. 8 that wants to communicate with a destination MP *X*.

In order to establish a secure route, source node S, destination node *X* and set of intermediate nodes F_1 that includes {A,B} and F_2 that includes {C,D} executes the route discovery process in the following way:

$$S \rightarrow * : MAC_{GTK} root(S), \{v_i, authpath(v_i)\}, \{PREQ-MF\}_{GTK} \quad (1)$$

$$F_1 \rightarrow * : MAC_{GTK} root(F_1), \{v_i, authpath(v_i)\}, \{PREQ-MF\}_{GTK} \quad (2)$$

$$F_2 \rightarrow * : MAC_{GTK} root(F_2), \{v_i, authpath(v_i)\}, \{PREQ-MF\}_{GTK} \quad (3)$$

$$X \rightarrow F_2 : MAC_{PTK}^{X,F_2} root(X), \{v_i, authpath(v_i)\}, \{PREP-MF\}_{PTK}^{X,F_2} \quad (4)$$

$$F_2 \rightarrow F_1 : MAC_{PTK}^{F_2,F_1} root(F_2), \{v_i, authpath(v_i)\}, \{PREP-MF\}_{PTK}^{F_2,F_1} \quad (5)$$

$$F_1 \rightarrow S : MAC_{PTK}^{F_1,S} root(F_1), \{v_i, authpath(v_i)\}, \{PREP-MF\}_{PTK}^{F_1,S} \quad (6)$$

The key management of 802.11s ensures that node *S* is equipped with one GTK that it shares with its neighbors and set of PTKs for communicating with each neighbor individually. Before broadcasting the PREQ, it first creates a Merkle tree with the leaves being the hash of mutable fields of PREQ message. *S* then creates a MAC on the root of the Merkle tree it just created. Then, S broadcasts message (1) which includes the MAC of the root created using the GTK, mutable fields v_is that need to be authenticated along with the values of its authentication path *authpath(* v_i *)*and encrypted PREQ message excluding the mutable fields.

Any of the neighboring nodes of *S*, after receiving the PREQ, tries to authenticate the mutable fields by hashing the values received in an ordered way, create a MAC on it using the shared GTK and comparing that with the received MAC value of the root. If the two values match, the intermediate MP is ascertain that the values are authentic and come from the same source that created the tree.

Let us consider, for example, that B receives a PREQ from its neighboring node S and wants to authenticate the value of the metric field M as shown in Fig. 9. According to our protocol, B and C should receive the value M along with the values of the authentication path of M in the Merkle tree such as U_H and U_{TF}. B and C can now verify the authenticity of M by computing $h(h(h(M)|| U_H)|| U_{TF})$ and a MAC on this value using the key GTK. It then compares the received MAC value with the new one, if it found a match, then it can assure that the value M is authentic and came from the same entity that has created the tree and computed the MAC on the U_{root}.

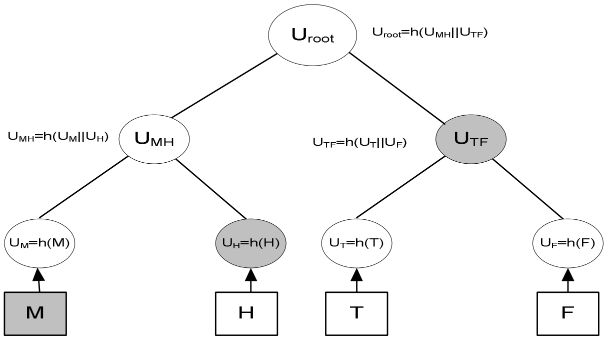


Fig. 9. Authentication path for the *metric* field in a Merkle Tree.

The intermediate nodes then update the values of the mutable fields (e.g., hop count, metric and TTL) and create Merkle trees from the modified fields. They also decrypt the non-mutable part of the PREQ message and re-encrypt it with their own broadcast key and re-broadcast (as shown in (2) and (3)) the PREQ message following the same principle. After receiving the PREQ, the destination MP updates the mutable fields; creates its own Merkle tree and unicasts a PREP message as in (4) using the same principle but this time it uses PTK instead of GTK. The PREP is propagated as (5) and (6) to the source MP in the reverse path created using PREQ and thus a secure forward path from the source to the destination is established.

2) Securing Proactive Mode: To accomplish security in proactive mode, we need to employ security in both Proactive RANN and Proactive PREQ mechanism.

In the *Proactive RANN* mode, the RANN message is broadcasted using the group transient key as shown in Eq. (7) – (9) to protect the non-mutable fields and authenticate the mutable fields (hop count, TTL and metric) using the Merkle tree approach. As there are only three mutable fields in the RANN message, a node requires generating a random number to construct the Merkle tree. After receiving the RANN message an MP that needs to setup a path to the root MP unicasts a PREQ to the root MP as per Eq. (10) – (12). Upon receiving each PREQ, the root MP replies with a unicast PREP to that node as described in Eq. (13) – (15).

$$R \rightarrow *: \mathrm{MAC}_{\mathrm{GTK}}\mathrm{Root}(R), \{v_i, \mathrm{authpath}\ (v_i)\}, \{\text{RANN-MF}\}_{\mathrm{GTK}} \tag{7}$$

$$F_1 \rightarrow *: \mathrm{MAC}_{\mathrm{GTK}}\mathrm{Root}(F_1), \{v_i, \mathrm{authpath}\ (v_i)\}, \{\text{RANN-MF}\}_{\mathrm{GTK}} \tag{8}$$

$$F_2 \rightarrow *: \mathrm{MAC}_{\mathrm{GTK}}\mathrm{Root}(F_2), \{v_i, \mathrm{authpath}\ (v_i)\}, \{\text{RANN-MF}\}_{\mathrm{GTK}} \tag{9}$$

$$D \rightarrow F_2: \mathrm{MAC}^{D,F_2}_{\mathrm{PTK}}\mathrm{Root}(D), \{v_i, \mathrm{authpath}\ (v_i)\}, \{\text{PREQ-MF}\}^{D,F_2}_{\mathrm{PTK}} \tag{10}$$

$$F_2 \rightarrow F_1\text{: } \text{MAC}^{F_2,F_1}_{\text{PTK}}\text{Root}(F_2),\ \{v_i,\ \text{authpath}\ (v_i)\},\ \{\text{PREQ-MF}\}^{F_2,F_1}_{\text{PTK}} \qquad (11)$$

$$F_1 \rightarrow R\text{: } \text{MAC}^{F_1,R}_{\text{PTK}}\text{Root}(F_1),\ \{v_i,\ \text{authpath}\ (v_i)\},\ \{\text{PREQ-MF}\}^{F_1,R}_{\text{PTK}} \qquad (12)$$

$$R \rightarrow F_1\text{: } \text{MAC}^{R,F_1}_{\text{PTK}}\text{Root}(R),\ \{v_i,\ \text{authpath}\ (v_i)\},\ \{\text{PREP-MF}\}^{R,F_1}_{\text{PTK}} \qquad (13)$$

$$F_1 \rightarrow F_2\text{: } \text{MAC}^{F_1,F_2}_{\text{PTK}}\text{Root}(F_1),\ \{v_i,\ \text{authpath}\ (v_i)\},\ \{\text{PREP-MF}\}^{F_1,F_2}_{\text{PTK}} \qquad (14)$$

$$F_2 \rightarrow D\text{: } \text{MAC}^{F_2,D}_{\text{PTK}}\text{Root}(F_2),\ \{v_i,\ \text{authpath}\ (v_i)\},\ \{\text{PREP-MF}\}^{F_2,D}_{\text{PTK}} \qquad (15)$$

Notations used in Eq. (7) – (15) are as follows. R is considered as the root MP and D is the MP that needs to setup a path to R. F_1 and F_2 are the intermediate nodes in the path. $\text{MAC}_k\text{Root}(X)$ represents the MAC of the Merkle tree's root created by the node X using a shared key k. {RANN/PREQ/PREP-MF} represents the routing information elements without the mutable fields. v_i and $authpath(v_i)$ denote the fields needed to be authenticated and the values assigned to the authentication path from v_i to the root of the tree, respectively.

Proactive PREQ mechanism is used to create paths between the root MP and the remaining MPs in the network proactively. Only the MP that is configured as a root MP would send proactive PREQ messages periodically. The proactive PREQ is also needed to be broadcasted to the MPs attached to the root MP encrypted using GTK of the root MP, the mutable fields (TTL, hop count, metric and per destination flag) of this PREQ should be authenticated in the intermediate MPs in the same way as discussed earlier. If an MP needs to update its path to the root MP, it unicasts a proactive PREP to the root MP. PREP is transmitted securely as in the case of PREP in on-demand mode.

6 Security and Overhead Analyses

In this section, we will analyze the proposed SLPS in terms of robustness against the attacks presented in Section 4 and also the overhead required for ensuring secure routing.

6.1 Security Analysis

1) Preventing Flooding Attack: In the proposed SLPS, a node can participate in the route discovery process only if it has successfully established a GTK and PTK through key distribution and authentication mechanism of 802.11s. Thus, it will not be possible for a malicious node to initiate a route discovery process with a destination address that is not in the network. Again, as the PREQ message is encrypted during transmission, a malicious node cannot insert new destination address.

2) Preventing Route Re-direction Attacks: The root cause of route re-direction attacks are modification of mutable fields in routing messages. These mutable fields are authenticated in each hop. If any malicious node modifies the value of a field in transit, it will be readily detected by the next hop while comparing the new MAC with the received one. It will find a miss-match in comparing the MACs and modified packet will be discarded.

3) Avoiding Formation of Routing Loops: Formation of routing loops requires gaining information regarding network topology, spoofing and alteration of routing message. As all the routing information is encrypted between nodes, an adversary will be unable to learn network topology by overhearing routing messages. Spoofing will not benefit the adversary as it will require authentication and key establishment to transmit a message with spoofed MAC. Moreover, fabrication of routing messages is detected by integrity check. So, the proposed mechanism ensures that routing loops cannot be formed.

6.2 Overhead Analysis

1) Computational Overhead: The computational overhead of a sender and a receiver can be given by:

$$\langle k \times h \rangle + m + e \text{ (sender)} \tag{16}$$

$$\langle a + 1 \rangle h + m + d \text{ (receiver)} \tag{17}$$

where, *k* is the number of hash operations required to form a Merkle tree. Cost of computing a hash function is defined by *h*, *m* is the cost involved in computing the MAC of the root, whereas *e* and *d* are encryption and decryption cost. To authenticate a particular value, a receiver need to compute the root by calculating (*a*+1) hash operations, where *a* is the number of nodes in the authentication path.

2) Communication Overhead: It is defined by the number of routing messages required to establish a secure path and given by Eq. (18), (19) and (20),

$$(n\text{-}1) \times broadcast + h \times unicast \quad (on\text{-}demand) \tag{18}$$

$$n \times broadcast + h \times unicast \quad (practive\ PREQ) \tag{19}$$

$$n \times broadcast + 2h \times unicast \quad (practive\ RANN) \tag{20}$$

where, *n* is the number of nodes in the network, *h* is the number of hops in the shortest path. The number of messages required for establishing a path in LPS is same as our proposed one. So, our protocol does not incur any extra communication overhead.

3) Storage Requirements: A node needs to store the number of fields that need to be authenticated, hashed values of the Merkle tree and the MAC of the root value. So, storage requirement of a node is given by Eq. (21).

$$\sum_{i=1}^{n} d_i + (k \times l) + S_M \tag{21}$$

Where, d_i is the size of a mutable field, *k* is the number of hashes in the Merkle tree, *l* is the size of a hashed value and S_M is the size of the MAC.

Table 2. Overhead Comparison

	Computation			Communication		Storage (bytes)
	Hash	MAC	Enc/Dec	Unicast	Broadcast	
LPS	0	0	0	h	n	20
SLPS	k	1	1	h	n	47

Table 2 summarizes the computation, communication and storage overheads required by a particular sender/receiver for both LPS and SLPS schemes. It shows that though the computation and storage requirements for the secure mechanism are slightly higher than the non-secure LPS scheme, the proposed SLPS scheme does not incur any extra communication overhead.

7 Performance Evaluation

In this section, we evaluate the performance of the proposed SLPS scheme. We use *ns*-2 [12] to simulate our proposed secure path selection approach and compare that with existing LPS. We have simulated 50 nodes in a 1500 x1500 m^2 area. We use 5 to 10 distinct source destinations pairs that are selected randomly. Traffic source are CBR (constant bit-rate). Each source sends data packets of 512 bytes at the rate of four packets per second during the simulation period of 900 seconds. The Performance metrics that considered are: i) **Packet delivery ratio:** Ratio of the number of data packets received at the destinations to the number of data packets generated by the CBR source, ii) **Control overhead (in bytes):** Ratio of the control overhead to the delivered data, iii) **end-to-end delay** for data packets, and iv) **path acquisition delay**, which is the time requires to establish a route for a source-destination pair.

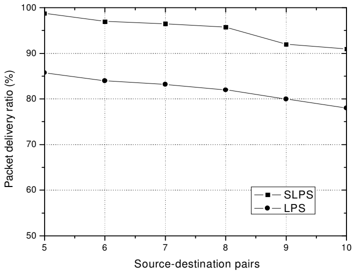


Fig. 10. Packet delivery ratio.

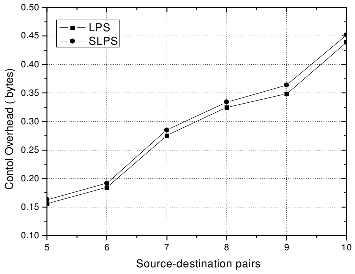


Fig. 11. Control packet overhead.

We assume that there are 10 nodes that are misbehaving and take part in the route discovery process and drop packets that they should forward. Since, in our secure routing approach, misbehaving nodes can not participate in the route discovery process and as a result it gives a better packet delivery ratio as shown in Fig. 10. On the other hand, though the number of control messages required to transmit for a route establishment is roughly the same, due to the addition of a MAC value, control packet overhead of the proposed scheme is slightly higher than the LPS scheme as shown in Fig. 11. But, this control overhead ensures higher security.

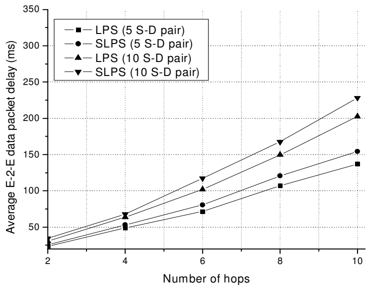


Fig. 12. End-to-end delay for data.

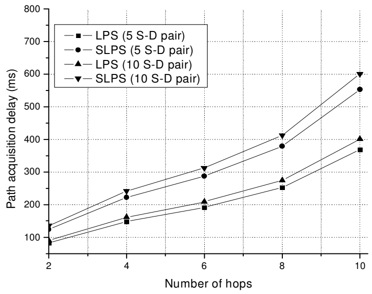


Fig. 13. Path acquisition delay.

Fig. 12 depicts that the average end-to-end delay of data packets for both protocols are almost equal. So, it is also evident that the effect of route acquisition delay on average end-to-end delay is not significant. Average route acquisition delay for the proposed SLPS scheme is much higher than that of the LPS mechanism as shown in Fig. 13. Because, in addition to normal routing operation of LPS, the proposed SLPS scheme requires computing hash and MACs values which require extra processing delay.

8 Conclusions

In this paper, we devise a secure path selection mechanism for wireless mesh networks that is gradually maturing to a point where it cannot be ignored when considering various wireless networking technologies for deployment. We have proposed SLPS, a secure extension of layer-2 routing specified in 802.11s. Our proposed mechanism takes into consideration the existing key hierarchy of 802.11s (so, there is no extra keying burden), identifies the mutable and non-mutable fields in the routing message, protects the non-mutable part using symmetric encryption and uses Merkle-tree approach to authenticate mutable information. We have shown that our protocol is robust against identified attacks and computationally efficient as it uses only symmetric key operations.

References

1. Akyildiz, I.F., Wang, X., Wang, W.: Wireless Mesh Networks: a Survey. In: Computer Networks, vol. 47, no. 4, (2005)
2. IEEE 802.11s Task Group, Draft Amendment to Standard for Information Technology Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking, IEEE P802.11s/D1.06, (2007)
3. Wang, X., Lim, A.O.: IEEE 802.11s Wireless Mesh Networks: Framework and Challenges. In: AdHoc Networks, doi:10.1016/j.adhoc.2007.09.003, pp. 1-15 (2007)
4. Merkle. R. C.: A Certified Digital Signature (subtitle: That Antique Paper from 1979). In: G. Brassard, ed., Advances in Cryptology – Proc. CRYPTO ’89 , volume 435 of LNCS, pp. 218–238. Springer-Verlang (1990)
5. Bahr, M.: Proposed Routing for IEEE 802.11s WLAN Mesh Networks. In: 2nd Annual International Wireless Internet Conference (WICON), Boston, MA, USA. (2006)
6. Bahr, M.: Update on the Hybrid Wireless Mesh protocol of 802.11s. In: Proc. of IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007. MASS pp.1-6 (2007)
7. Hu, Y-C., Perrig, A., Johnson, D. B.: Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In: Proc. MobiCom ’02, Atlanta, GA, (2002)
8. Perrig, A., Canetti, R., Tygar, J.D., Song, D.: Efficient Authentication and Signing of Multicast Streams over Lossy Channels. In: Proc. of IEEE Symposium on Security and Privacy, 2000. pp.56-73 (2002)
9. Gergely, A, Buttyan, L., Vajda, I.: Provably Secure On-demand Routing in Mobile Ad Hoc Networks. In: IEEE transactions on Mobile Computingm Vol.5 No.11, pp.1533-1546 (2006)
10. Zapata, M.G., Asokan, N.: Securing Adhoc Rouring Protocols. In: Proc. of ACM Workshop of Wireless Security(Wise), pp.1-10 (2002)
11. Sangiri, K., Dahil, B.: A Secure Routing Protocol for Ad Hoc Networks. In: Proc. of 10th IEEE International Conference on Network Protocols (ICNP’02)
12. The Network Simulator – ns-2, http://www.isi.edu/nsnam/ns/index.html
13. Lim, A.O., Wang, X., Kado, Y., Zhang, B.: A Hybrid centralized Routing Protocol for 802.11s WMNs. In: Journal of Mobile Networks and Applications, Springer, (2008)