DEFENDING AGAINST WORMHOLE ATTACK IN MULTI-HOP WIRELESS MESH NETWORKS

P. Subhash [1] , S. Ramachandram [2]

[1] Department Of CSE, Jyothishmathi Institute of Technological Sciences, Karimnagar, Telangana, India

[2] Department Of CSE, University College of Engineering, Osmania University, Hyderabad, Telangana, India

ABSTRACT: In Wireless Mesh Networks (WMNs), many of the existing routing protocols are vulnerable to various types of attacks. One such attack that causes severe impact on a wireless mesh network is the Wormhole attack. Wormhole attack is a type of tunneling attack, in which the network messages are captured at one end and transmitted to other end through a low-latency link called virtual tunnel. In this paper, we propose a security mechanism to defend against byzantine wormhole attack on Hybrid Wireless Mesh Protocol (HWMP), which is a mandatory path selection protocol in multi-hop wireless mesh networks. The investigated mechanism prevents the formation of wormholes during the route discovery phase in an on-demand routing protocol of WMNs. Analysis and simulation of the proposed mechanism are performed in Omnet++,a discrete event network simulator. The proposed solution is simple and software based, it does not require each node in the network to be equipped with a specialized hardware.

KEYWORDS: Byzantine Wormhole attack; Wireless Mesh Networks; HWMP; Security Mechanisms.

I. INTRODUCTION

Wireless Mesh Networks (WMNs) have become an emerging technology to meet challenges of next generation networks and offers cost-effective solutions to the service providers. A typical WMNs consist of mesh routers and mesh clients. In WMNs, mesh routers are static (or having minimum mobility) and mesh clients are either static or highly mobile. Mesh routers can form mesh backbone network that can be connected to the internet via mesh gateway routers.WMN has many advantages such as low-setup cost, extended coverage and also offer flexible and reliable services, meeting all these requirements and providing security is one of the big challenging task because the open nature of the wireless medium itself is susceptible to various types of attacks [W08]. The numerous application scenarios [AWW05] of WMNs include home networking, community networks, enterprise networks, backhaul support for cellular networks, etc. WMNs can be classified into three groups based on their architecture and design: One-tier mesh networks,Two-tier mesh networks and Hybrid wireless mesh networks. One-tier mesh networks are No-Infrastructure mesh networks, Two-tier mesh networks are infrastructure mesh networks consist of mesh backbone routers, which can perform the routing functionality and communicate with clients, finally, Hybrid mesh networks offer functionalities of both one-tier and two-tier mesh networks. Figure 1 shows a typical architecture of wireless mesh networks.

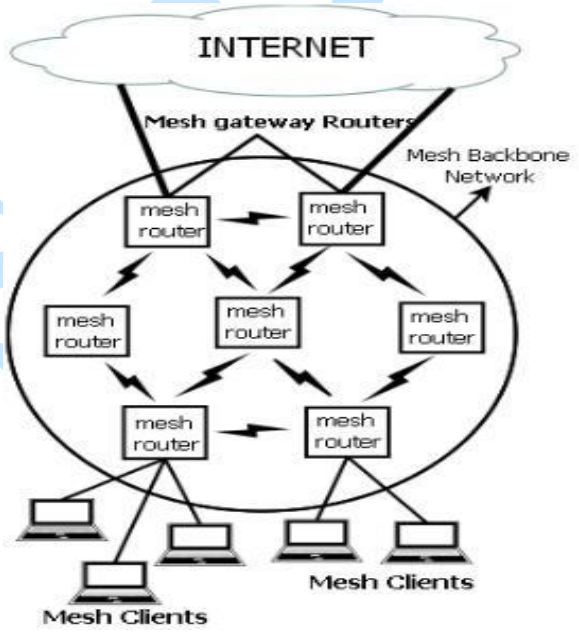

Figure 1: Network Architecture of WMN

Byzantine wormhole attack is a special type of a wormhole attack, where adversary nodes in the network collude to establish a low-latency link between them. This channel can be an out-of-band high-speed communication link or can employ in-band tunneling approach to bypass several intermediate nodes. This wormhole link is usually established between two colluding nodes located far away in the network. Once established, the wormhole attracts lots of traffic as it advertises much better link metric than any other paths in the network. The wormhole nodes can then launch various kinds of denial of service (DoS) attacks that severely affect the performance of the network. The main aim of the proposed solution is to significantly reduce the impact of the wormhole attack in wireless mesh networks. The part of this work is published in [SR13]. The

wormhole attack can also be launched even without compromising any node in the network [PS04].

Several classes of variant secure routing techniques in the field of WMNs have been investigated. Secure routing is considered to be one of the most challenging issues in WMNs as they are suffering from various types of vulnerabilities. The proposed solution is based on virtual coordinate system to defend against FRI-Attack in WMNs for on-demand hop by hop routing protocols like HWMP (Hybrid Wireless Mesh Routing) protocol. The HWMP is the default routing protocol for path selection in WMNs according to IEEE 802.11s [***] standard to provide interoperability between devices of different vendors. HWMP works on layer 2 with Mac addresses and uses airtime metric [Bah06] for the path selection.

Depending upon the configuration, HWMP uses two modes of operations.On-demand mode is used when there is no root mesh station configured. On-demand mode can also be used, when it offers a better path to the target even if there is a root mesh station configured.The proactive tree building mode is used when there is a root mesh station configured. In this mode either proactive PREQ or RANN mechanism is used by the root mesh Station. In HWMP, proactive mode and on-demand modes are used concurrently to achieve higher throughput.

ATLM metric is used in HWMP to establish an efficient radio aware path. ATLM is referred as the amount of channel resources consumed by transmitting the frame over a particular link.

$$C_a = [O_{ca} + O_p + \frac{B_t}{r}]\frac{1}{1-e_{pt}}$$

The airtime cost for each pair wise link C_a is calculated in terms of the modulation rate (r) and bit error rate e_{pt} for a test frame of B_t size. Where O_{ca} the channel access overhead is, O_p is the protocol overhead. O_{ca}, O_p and B_t are constants defined for each 802.11 modulation type.

II. RELATED WORK

Most of the existing wormhole defense mechanisms have been proposed with the support of an additional hardware, clock synchronization, accurate time measurements, etc.

Hu et al. proposed the concept of packet leashes to detect wormholes in wireless networks [HPJ03]. It uses two types of packet leashes, one is geographic leashes and another one is temporal leashes. But this approach requires GPS and tightly synchronized clocks.

Hu and Evans proposed a cooperative protocol [HE04] in which directional information is shared among nodes to prevent wormhole attack. This mechanism does not require clock synchronization and location information, but it requires additional hardware.

Van Tran and Xuan Hung proposed a transmission time based mechanism [T+07] for detecting wormhole attacks (TTM). This method calculates every Round Trip Time (RTT) between two successive nodes along the route. Each node in the path will calculate RTT between it and the destination, this value will be sent back to the source. Wormholes can be identified based on the RTT value as the RTT value between two fake neighbors is greater than the RTT value between two real neighbors.

Choi and Kim [C+08] proposed wormhole attack prevention algorithm (WAP). All the nodes will monitor its neighbor's behavior when they send RREQ messages to the destination with the help of neighbor list. If the source does not receive a RREP message within a stipulated time, it can detect the presence of the wormhole. Once wormhole is detected, source node records them in its wormhole node list. WAP can able to detect both the hidden and exposed attacks without requiring special hardware. This method does not fully support DSR as it is based on end-to-end signature authentication of routing packets.

DeWorm protocol [HKT09] proposed by Thaier et.al. uses routing discrepancies between neighboring nodes along a path from a source to the destination to detect wormhole attacks. This protocol is simple and localized. This method needs no special hardware, location (or) synchronization and it can detect physical layer wormholes.

WARP is a Wormhole Avoidance Routing Protocol [Su10], considers link-disjoint multipath during path discovery, but eventually uses only one path for data transmission. WARP avoids wormhole attacks by anomaly detection and it is based on adhoc on-demand routing protocol (AODV) [PRD04]. Every node in WARP maintains the anomaly values of its neighbors in its routing table. WARP enables the neighbors of the wormhole nodes to discover that the wormhole nodes have an abnormal path attraction

Lv, Guoyuan et al [G+13] proposed a detecting and defending against wormhole attack based on timer ruler, in which all the neighboring nodes must send routing packets following its pre designed time ruler and the wormhole attack can be detected by the sending time ruler or receiving time ruler.

III. NETWORK AND SECURITY MODEL

A. Network Model

We consider a typical WMN architecture, where a set of mesh routers (MR's) form the backbone of the WMN. Few of these MR's are designated with an additional functionality and act as gateway nodes by

connecting to the Internet. Mesh clients (MC's) are typical wireless clients connected to specific MR's with access point functionality. We also assume that all communication links are bi-directional. This is required by most of the wireless MAC protocols, including 802.11s, to operate correctly.

B. Security Model and Considered Attacks

We consider that a public-key infrastructure administred by a Certificate Authority(CA) exists in the network [IHH09]. PTK and GTK are used for authenticating unicast and broadcast messages respectively. Before initiating a route discovery process, all the MPs authenticate its neighboring MPs, sends its GTK (Group Transient Keys) and establish PTK(Pairwise Transient Keys) through key distribution process. GTK is used for securing broadcast messages such as path request (PREQ), route announcement (RANN) and priority path request (PPREQ). PTK is used for securing unicast messages such as path reply (PREP) and proactive path reply (PPREP). We consider only the source and destination to be trusted, and assume that there exists a non-adversarial path between source and destination. Information elements are accepted and process-ed from mesh STA's that are authenticated using authenticated mesh peering exchange protocol (AMPE).

Intermediate nodes on the path between the source and destination may collude to establish wormhole links between them. Such nodes can then launch various kinds of packet dropping attacks such as greyhole and blackhole. A wormhole link can essentially bypass all the nodes in between them to project a path formed through wormhole as the best of the available paths. The goal of our protocol is to detect byzantine wormhole links and thus avoid all packet dropping and metric manipulation attacks.

IV. PROPOSED MECHANISM TO PREVENT BYZANTINE WORMHOLE

In order to detect and prevent a path being established through a byzantine wormhole link, we make use of large discrepancies in hop-count and metric reported by various paths, during the route discovery process. Algorithm.1 and Algorithm.2 describes the route discovery process of on-demand and pro-active routing protocols respectively. We assume that there exist a path that does not contain any adversaries between source and destination, otherwise secure routing would be impossible. We make use of digital signatures to prevent intermediate nodes from tampering with the accumulated metric. Our proposed mechanism requires only nodes that are in multiple of two-hops away from the source S initiating the route discovery process to sign the metric field separately. This essentially restricts the number of nodes required to sign the metric to n/2 on a path of n nodes. The main motivation behind employing explicit signatures on metric field is to prevent wormhole nodes from manipulating accumulated metric on the path till the wormhole node.Moreover, as the route discovery process requires all two-hop nodes to explicitly sign the metric field, the wormhole link is effectively narrowed down to a single link, thus significantly reducing the influence of a wormhole. The proposed mechanism maintains neighborhood relations with all its two-hop neighbors and further processes messages generated only by its valid two-hop neighbors. The proposed mechanism can be separated into two distinct processes, route discovery process and wormhole detection process.The flow chart of the proposed mechanism is shown in figure 3.

A. Route Discovery Process

The Hybrid Wireless Mesh Protocol (HWMP) has combined the flavor of reactive and proactive routing strategy by employing both on-demand path selection mode and proactive tree building mode. On-demand mode allows two MPs to communicate using peer-to-peer paths. This mode is mainly used by nodes that experience a changing environment and when there is no root MP configured. On the other hand, proactive tree building mode can be an efficient choice for nodes in a fixed network topology. The mandatory routing metric used in HWMP is the airtime metric [***] that measures the link quality (e.g. amount of channel resource consumed by transmitting a frame over a particular link). In HWMP, both on demand and proactive mode can be used simultaneously. The proposed mechanism works for both the reactive and proactive strategies with little modifications in the wormhole prevention process.

In on-demand mode, the path selection decision is made by the destination by choosing a path that offers best airtime out of the set of available paths. Each node receives multiple copies of same PREQ but a node processes a later received PREQ only if the metric reported by it is better than the previously received metric. But, to increase the number of potential paths in our proposed mechanism, each node broadcasts all the PREQ's that it receives. The proposed algorithm is based on the assumption that the length of the wormhole is at least 2R where R is the range of a node. Each node maintains neighborhood relations with all its two-hop neighbors. This is facilitated at the MAC layer or at the network layer during the route discovery process.

Algorithm 1: On-demand Route Discovery Process

1: Carried out by source node S initiating the route Discovery process
2: Broadcast $\{P\ REQ, N/A, S, 1, 0\}_S\{S, 1, 0\}_S$
3: Carried out by an intermediate node receiving the PREQ
4: if (FLAG == 1) then
5: Set FLAG status to 0
6: Update the METRIC field and re-broadcast the PREQ
7: end if
8: else
9: if (FLAG == 0) then
10: Set FLAG status to 1
11: Set METRIC field in PREQ to 0, append t he PREQ with an authenticated message containing ADDR, F LAG, $Metric_I$
12: end if

Public and private key-pairs exist between each node and all its two-hop neighbors. Whenever a source mesh STA wants to discover a route to destination mesh STA using the on-demand mode, it broadcasts a PREQ with the target mesh STA specified in the list of targets and the metric field initialized to 0. A mesh STA that receives a new PREQ, creates or updates its path information to the originator mesh STA and propagates the PREQ to its neighbor peer mesh STAs. The PREQ is accepted if it contains a greater HWMP sequence number, or the HWMP sequence number is the same as the current path and the PREQ offers a better metric than the current path. The PREQ shown in figure 2 is modified to include the address of the previous hop (pre-cursor STA) that the PREQ has traversed and a special FLAG bit that allows nodes to determine their relative position from source.
The PREQ is further extended with an authenticated extension that includes the address of the signing node, the flag-bit status and the accumulated metric computed by that node. The authenticated extension of PREQ is appended by only nodes that are in multiple of 2-hops away from the source. The FLAG bit in the PREQ allows nodes to determine their role in processing the PREQ. If the status of the FLAG bit is 0,then nodes append the PREQ with an authenticated field as specified else they process the PREQ normally. The PREQ is represented using the following notation {PREQ, PrevNode, Tr.Node, FLAG, Metric$\}_N$ {ADDR, FLAG, Metric $\}_N$

Element ID	Length	Flags	Hop Count	Element TTL	PREQ ID	Org.Mesh STA Addr.	Org. HWMP Seq.NO
Org.Ext Addr.	Life Time	Metric	Target Count	Pre target fields #1	Target Address #1	Target HWMP Seq.No.	.....

Figure 2: PREQ Element

HWMP employs two mechanisms for proactively disseminating path selection information for reaching the root mesh STA. The first method uses a proactive Path Request (PREQ) element and is intended to create paths between the root mesh STA and all mesh STAs in the network proactively. That is, a node interested in creating a forward path towards the root replies to the proactive PREQ with a PREP. The second method makes use of a Root Announcement (RANN) element and is intended to distribute path information for reaching the root mesh STA but there is no forwarding information (routing entry) created. A mesh STA configured as root mesh STA would send either proactive PREQ or RANN elements periodically.

Algorithm 2: Proactive Route Discovery Process

1: Carried out by root node R initiating Route Discovery Process
2: Broadcast $\{P\ P\ REQ, N/A, S, 1, 0\}R\ \{S, 1, 0\}R$
3: Carried out by an intermediate node receiving the PPREQ
4: if (FLAG == 1) then
5: Set FLAG status to 0
6: Update the METRIC field and re-broadcast the PPREQ
7: end if
8: else
9: if (FLAG == 0) then
10: Set FLAG status to 1
11: Set METRIC field in PREQ to 0, append the PPREQ with an authenticated message Containing ADDR, F LAG, $Metric_I$
12: end if

The Proactive PREQ mechanism begins with a proactive PREQ element broadcasted by the root mesh STA and the target only flag set to 1. The PREQ contains the path metric set to 0 and an HWMP sequence number. The proactive PREQ is sent periodically by the root mesh STA, with increasing HWMP sequence numbers. A mesh STA receiving a proactive PREQ creates or updates its forwarding information to the root mesh STA, updates the fields of the PREQ accordingly and then transmits the updated PREQ.
Each mesh STA may receive multiple copies of a proactive PREQ, each traversing a unique path from the root mesh STA to the mesh STA. A mesh STA updates its current path to the root mesh STA if and only if the PREQ contains a greater HWMP sequence number, or the HWMP sequence number is the same as the current path and the PREQ offers a better metric than the current path to the root mesh STA. If the proactive PREQ is sent with the "Proactive PREP" bit set to 0, the recipient mesh STA may send a proactive PREP. A proactive PREP is necessary, for example, if the mesh STA has data to send to the root mesh STA, thus requiring the establishment of a forward path from the root mesh STA). During the time the forward path is required,

the recipient mesh STA shall send a proactive PREP even if the "Proactive PREP" bit is set to 0. If the PREQ is sent with a "Proactive PREP" bit set to 1, the recipient mesh STA shall send a proactive PREP. The proactive PREP establishes the path from the root mesh STA to the mesh STA.

In the proactive RANN mechanism, the root mesh STA periodically propagates a RANN element into the network. Nodes that intend to establish a route to the root mesh STA sends an individually addresses PREQ via the mesh STA from which it received the RANN. The root mesh STA then sends a PREP in response to each PREQ.The individually addressed PREQ creates the reverse path from the root mesh STA to the originator mesh STA, while the PREP creates the forward path from the mesh STA to the root mesh STA. Typically, the information contained in the RANN is used to disseminate path metrics to reach the root mesh STA, but reception of a RANN does not establish a path.

B. Wormhole Detection Process

The wormhole detection process shown in Algorithm.3 thrives on the fact that the path received through a wormhole advertises much better metric than the other paths free of malicious nodes.Each intermediate node on the potential path towards the destination runs the wormhole detection process to verify the genuinity of the advertised paths. The signature extensions received in the PREQ allows an intermediate node I to determine and compare the cost (metric) incurred by its two-hop neighbor in reaching the particular neighbor I. As the proposed mechanism requires nodes to
generate PREQ's with a valid pre-cursor mesh STA, the nodes establishing the wormhole link need to advertise the node at the other end of a wormhole as a neighbor. That effectively limits the capability of a wormhole to a single hop. The intermediate node I that receive multiple copies of PREQ with similar PREQ-ID, compares the length of a reported wormhole path with other received paths. This comparison of paths is restricted depending on the number of signed extensions in the PREQ.

Without loss of generality, a wormhole path effectively registers less signed extension fields when compared to other paths as it bypasses all the intermediate nodes in between the wormhole link. The metric value present in the last explicitly signed field in the PREQ arrived through a wormhole path is compared with other alternate paths.For the proposed mechan- ism to prevent nodes from establishing paths through wormholes, it requires the existence of a path free of adversaries. The wormhole link metric and hop-count is compared with the metric reported through other paths. If the difference in the length of the other alternate path and the wormhole is greater than (>2), then it is considered to be wormhole.The intermediate node also estimates the value of R, the airtime metric to its one-hop nodes and compares it with the metric reported in wormhole.The value of two signifies the fact that, to reach a distance of one-hop as claimed by the worm- hole, the other alternate paths require more than 2-hops and the difference in metric is greater than 2R. As, the length of the wormhole increases the confidence level on the detection process exponentially increases.

Algorithm 3: Wormhole Detection Process

```
1:  Carried out by each node involved in the Route Discovery Phase
2:  On receiving a duplicate copy of a PREQ a node Compares the best METRIC (MS) with the METRIC obtained in the rest of the obtained PREQ's (MC)
    //MS is the metric under suspicion and MC are the set of candidate METRICS
3:  if (PREQ_METRIC == 0) then
4:  Compare the METRIC signed by the latest transmitter after adding the CURRENT-HOP METRIC with the rest of the PREQ's METRIC
5:  end if
6:  else
7:  if (PREQ_METRIC!= 0) then
8:  Compare the METRIC received in PREQ after adding the CURRENT-HOP METRIC with the rest of the PREQ's METRIC
9:  end if
10: for each MC do
11:   if ((MC - MS) ≥2R) then
12:   Wormhole Detected
13:   Node through which the METRIC received is MS
        is the source of wormhole
14:   Broadcast a WARNING message on the identified
      nodes
15:   end if
16: else
17:   No wormhole detected
18: break
19: end for
```

V. EXAMPLE SCENARIO

In order to understand the wormhole detection mechanism, consider the following example network scenario shown in figure 4. The wormhole detection algorithm runs on every node in the network, but at node P, it prevents the formation of wormhole route received from a malicious node M. Node P receives multiple PREQ elements from its neighboring nodes, it accepts the PREQ elements from only its valid 2-hop neighbors. In this scenario, node E and node M are assumed to be colluding nodes to form byzantine wormhole link.

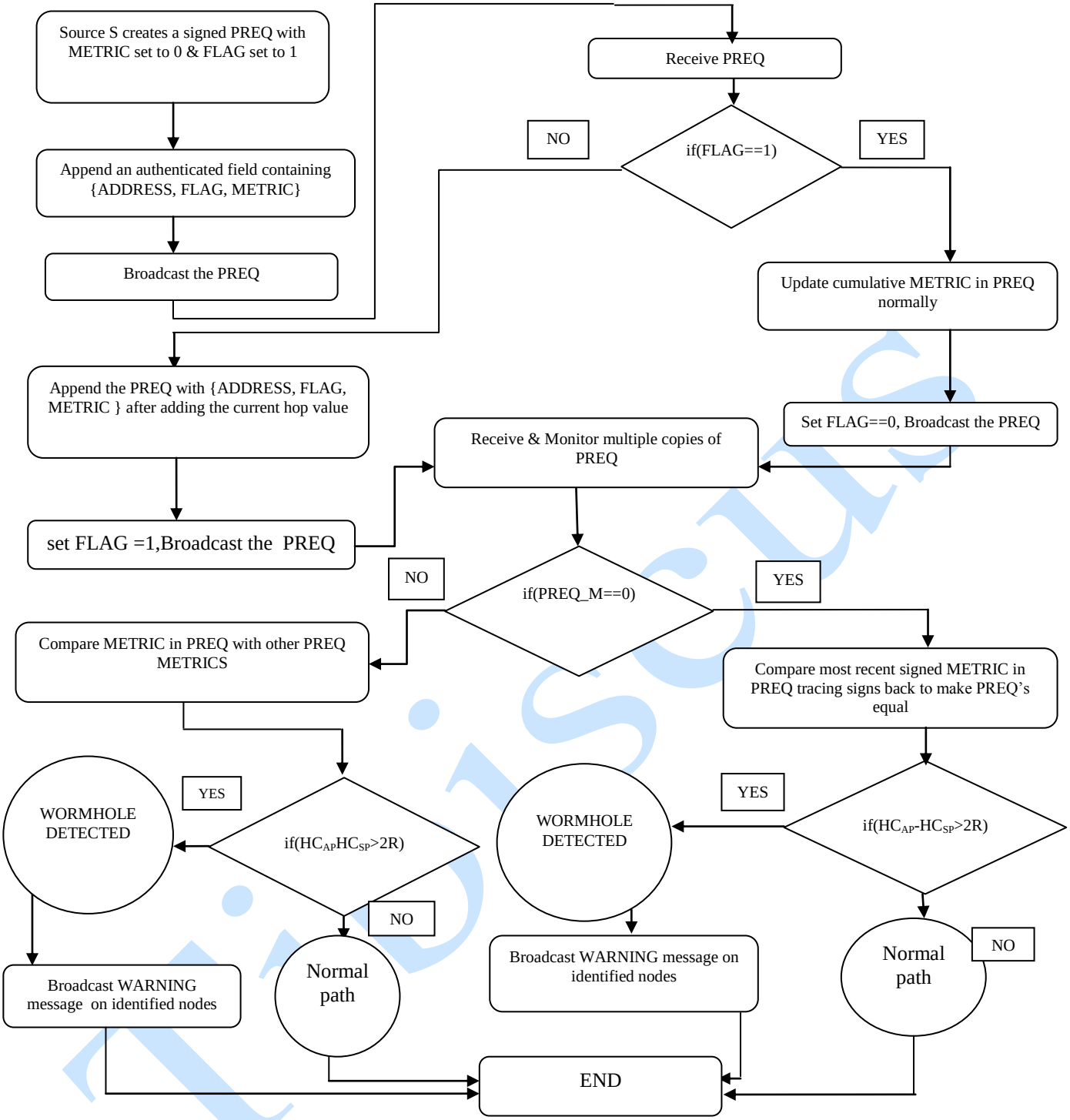

Figure 3: A flow chart of the proposed mechanism

Node P receives the PREQ element from node M, offering better metric and consisting a less number of signatures as all the traffic is bypassed through a virtual tunnel between colluded nodes. Node P also receives the PREQ element from node O, consisting more no of signatures as this is free of wormhole link.

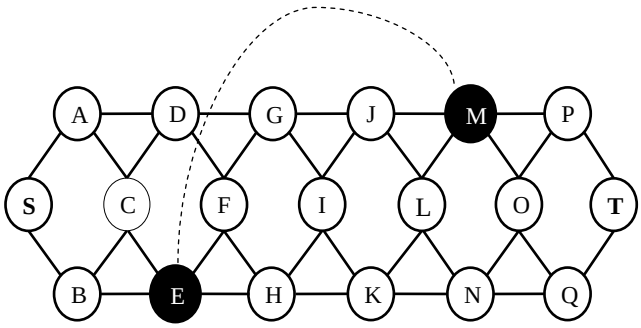

Figure 4: Example wormhole attack scenario

The process of detecting wormhole path is carried out by node P, based on the observation of large discrepancy value between suspicion metric (Metric value reported from node M) and Candidate metric (Metric value reported from node O), broadcast a warning message on the identified nodes. Thus, avoiding the formation of wormhole links during the route discovery phase of an on-demand routing protocol in WMNs.

VI. SECURITY ANALYSIS

The goal of the proposed mechanism is to significantly lower the impact of wormhole link by not allowing nodes to manipulate the metric of a path beyond a certain limit. Manipulation of the routing information allows the colluding nodes to control the forwarding topology such that traffic is forwarded over path containing the attacker nodes. The use of digital signatures to specifically sign the metric field, does not allow the colluding nodes to manipulate the metric of an accumulated path beyond the wormhole link. The single link that the colluding nodes can manipulate is in fact the length of the wormhole. The wormhole detection algorithm allows a node receiving multiple PREQ's to compare the length of the received paths. The comparison is restricted to a sub-path of maximum length 3-hops. The proposed mechanism relies on the ability to not allow colluding nodes to decrease the metric and in a few cases the malicious nodes in fact artificially increase the metric to avoid being detected. The success probability of the wormhole detection process depends on the length of the wormhole. As the length of the wormhole increases, its detection probability increases exponentially. The security analysis lies in showing that the colluding nodes cannot manipulate the proposed mechanism and launch a wormhole attack resulting in various DoS attacks.

*A. **Route Discovery***

During route discovery, nodes broadcast the PREQ element after appropriately processing its fields. Each node, depending on its relative position from the original source appends the additional signed metric field to the PREQ. Each node that is in multiples of 2-hop from the source signs an additional field containing the signing node address, FLAG status and the metric and appends it to the PREQ. This relative position is determined with the help of the flag bit present in the PREQ. A node that receives the PREQ, checks the status of the flag bit to determine whether it needs to specifically append an additional field, or simply update the metric field in PREQ. According to the proposed mechanism, the colluding nodes on a given path can be either positioned at (2Sn) or (2Sn +1) hops away from the source.

1) Case($2S_n$)

The proposed mechanism does not allow nodes involved in the path selection process from decrementing the accumulated metric without being detected. In this specific case, where the wormhole link begins at a multiple of 2-hop from the source, the attacker nodes can only influence the metric of at most three links. As, the proposed mechanism requires every alternate node to sign the metric field explicitly beginning from the source, in this case the node positioned at the beginning of the wormhole link needs to explicitly sign the metric field. Therefore, such node before explicitly signing the metric field, needs to update the cumulative metric in PREQ and set the metric field in actual PREQ to 0. Each explicitly signed metric field, contains the cumulative metric of 2-hops. Therefore, the colluding nodes lying on multiple of 2-hops away from the source, can only manipulate metric up to a maximum of 3-hops including the wormhole link.

2) Case($2S_n + 1$)

In this specific case, where the wormhole link does not begin at a multiple of 2-hop from the source, the attacker nodes can only influence the metric of at most two links. As, the pre-cursor node positioned at 2Sn to the wormhole node explicitly signs the metric field and sets the metric in PREQ to 0, the wormhole node can only manipulate the metric of at most two links including the wormhole link.

*B. **Wormhole Detection Process***

The proposed wormhole detection process depends on the large discrepancies between a wormhole path and normal path. The two-hop neighborhood information maintained by each node allows them to accept and process messages form only registered two-hop nodes. The two-hop signing approach restricts the wormhole nodes from forging large distances on a selected path. As, each node in the proposed mechanism continuously verifies the 2-hop sub-path of all received paths, the wormhole path that bypasses several in between nodes and projects the wormhole link as a single link path, it is detected by the nodes monitoring the paths. The correctness of the approach lie in the fact that, the wormhole nodes try to increase the metric to avoid being detected which in fact lowers the probability of that wormhole path being selected.

3) Case($2S_n$)

In this particular case, if wormhole node manipulates the metrics maximum possible links which in this case is three, the probability of its detection increases as only part of the path's (sub-path) length are compared. The amount of discrepancy is more evident when shorter sub-paths are compared. Any alternate path between the two-points under comparison does not deviate beyond the sensitivity parameter. Therefore, the wormhole nodes either try to inflate the metric or are forced to manipulate only the wormhole link metric. Wormhole nodes cannot inflate the metric beyond a certain limit as the maximum metric of a single hop link can be obtained from the worst path received that is in turn free of malicious nodes.

4) Case($2S_n + 1$)

In this particular case, a wormhole node can manipulate an additional link under its control, apart from the wormhole link. If the length of the wormhole if long, in a similar way as stated above, the amount of discrepancy would become more evident when shorter sub-paths are compared within a two-hop distance. Any alternate path between the two-points under comparison does not deviate beyond the sensitivity parameter. Therefore, the wormhole nodes in fact avoid skipping in between nodes to prevent wormhole link from becoming more evident. This approach to break down paths into shorter sub-paths and explicitly signing of metric fields significantly lowers the impact of a wormhole and in most of the cases they are naturally avoided as the amount of discrepancy would be kept to a minimum when a shorter wormhole link is not detected.

VII. SIMULATION RESULTS

In this section, we present the simulation results of the proposed wormhole detection mechanism. Specifically, we evaluate the performance of the protocol in the presence of malicious nodes and also for the additional overhead incurred to provide security. The experiments were carried out on OMNeT++ 4.2.1, a discrete event network simulator [***11]. The network set-up consists of a varying number of MRs (50-200) for different experiments, forming the mesh backbone. The transmission range of a MR is set to 100 m. MRs implement the 802.11s MAC protocol with a channel data rate of 54Mbps. Source (or root of the tree), and destination are selected at random for each experiment. Figure 5 shows the performance of the proposed mechanism in the presence of varying number of malicious nodes, in terms of percentage of packet delivered. The principle goal of these malicious nodes is to disrupt network services by dropping data packets. The performance is compared with HWMP. The main aim of this experiment is not to highlight the PDR achieved by the proposed scheme but to showcase the loss of data due to the presence of malicious nodes in the network.

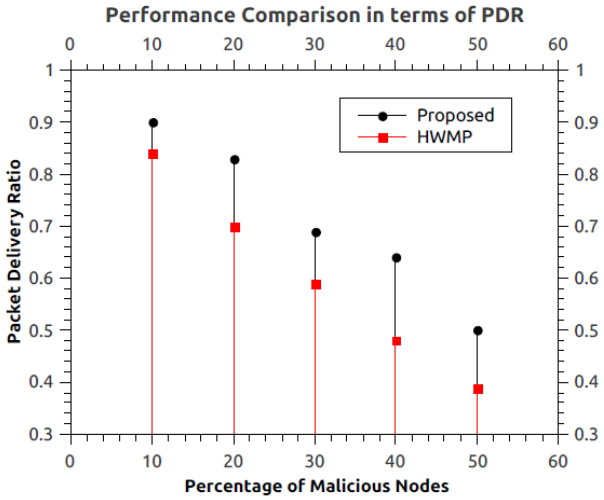

Figure 5: Performance Comparison in terms of PDR

Our later experiments focus on the overhead incurred by the proposed defense mechanism due to its security enhancements. First, we study the route creation overhead (in terms of additional bytes per packet) incurred for varying the average length of a route. The network setup comprised of 100 MRs spread over 1000 m^2. Figure 6 and figure 7 shows the overhead in comparison to HWMP. The increase in packet size is mainly to accommodate the additional addresses for detecting a route traversing a wormhole link.

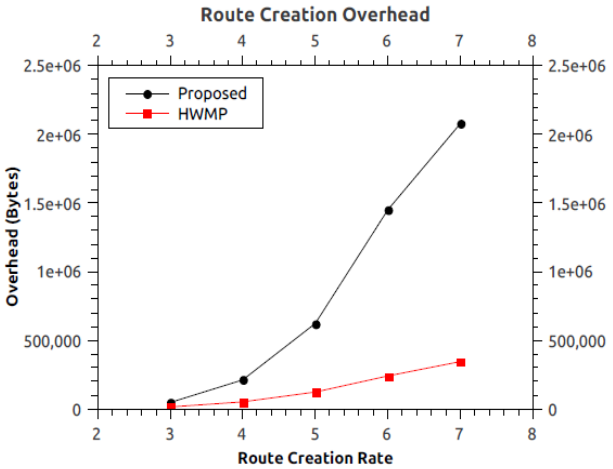

Figure 6: Route creation overhead for varying route creation rate

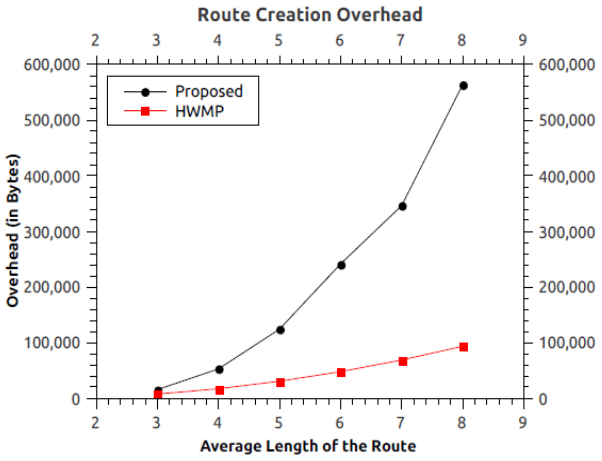

Figure 7: Route creation overhead for varying average length of a route

VIII. CONCLUSION

In this paper, we proposed an efficient mechanism to prevent the formation of byzantine wormholes in WMNs. This mechanism is simplistic and it does not rely on additional resources like GPS systems. The use of digital signatures limits malicious nodes from decrementing a path's metric beyond certain extent and in turn reduces the impact of wormhole attack. The proposed mechanism requires only alternate nodes to sign the metric field, thus constrains generation of excessive overhead. The wormhole detection process relies on discrepancies in length of normal paths and paths received through a wormhole link. As, each node only monitors immediate 2-hop sub-path's on a received path, the detection mechanism, accurately detects and prevents a wormhole link from being established. The accuracy with which a wormhole link can be detected depends on the length of a wormhole. It exponentially increases with an increase in the length of a wormhole link.

REFERENCES

[AWW05] **Ian F. Akyildiz, Xudong Wang, Weilin Wang** - *Wireless mesh networks: A survey*, Computer networks and ISDN systems, 2005.

[Bah06] **Michael Bahr** - *Proposed routing for IEEE 802.11s WLAN mesh networks*. Proceedings of the 2nd annual international workshop on Wireless internet. ACM, (2006).

[C+08] **S. Choi, D. Y. Kim, D.H. Lee, J. L. Jung** - WAP: Wormhole Attack Prevention Algorithm in Mobile Ad hoc Networks, In Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing. Pages343-348, 2008.

[G+13] **Lv Guoyuan, Yiming Wang, Canyan Zhu, Rong Chen, Lujie Wang** - *A Detecting and Defending Method of Wormhole Attack Based on Time Ruler*. 2013.

[HE04] **L. Hu, D. Evans** - *Using directional antennas to prevent wormhole attacks*, in Network and Distributed System Security Symposium (NDSS), San Diego, 2004.

[HKT09] **T. Hayajneh, P. Krishnamurthy, D. Tipper** - *DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad hoc Networks*, In Proceedings of Third International Conference on Network and System Security, Pages 73-80, October 2009.

[HPJ03] **Y. Hu, A. Perrig, D. Johnson** - *Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks*, In Proceedings of the Twenty Second IEEE International Conference Computer and Communications, Volume 3, Pages 1976-1986, April 2003.

[IHH09] **Md Shariful Islam, Md Abdul Hamid, Coong Seon Hong** - *SHWMP: A Secure Hybrid Wireless Mesh Protocol for IEEE 802.11s Wireless Mesh Networks*, Transactions on Computational Science VI Lecture Notes in Computer Science, Volume 5730, pp. 95-114, Springer 2009.

[PS04] **T. Park, K. Shin** - *LISP: A Lightweight Security Protocol for Wireless Sensor Networks*, in Proceedings of ACM transaction on Embedded Computing systems, August, 2004.

[PRD04] **C. E. Perkins, E.M. Royer, S. R. Das** - *Ad hoc On-demand Distance Vector (AODV) Routing*, IETF Internet Draft. MANET Working Group; Jan 2004.

[Su10] **M. Y. Su** - *WARP: A Wormhole Avoidance Routing Protocol by Anomaly Detection*, in Mobile Ad hoc Networks, Computers and Security, Volume 29, Issue 2, Pages 208-224, March 2010.

[SR13] **P. Subhash, S. Ramachandram** - *Preventing Wormholes in Multi-hop Wireless Mesh Networks*. Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on, IEEE, 2013.

[T+07] **P. V. Tran, L. X. Hung, Y.-K. Lee, S. Lee, H. Lee** - *Ttm: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks*, in In Proc. of IEEE CCNC,2007.

[W+08] **W. Zhang, Z. Wang, S. K. Das, M. Hassan** - *Security Issues in Wireless Mesh Networks*, In Book, Wireless Mesh Networks: Architectures and Protocols, Springer 2008.

[***] *IEEE P802.11s/D5.0 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Amendment 10: Mesh Networking.

[***11] The OMNeT++ Network Simulator: http://www.omnetpp.org. Accessed 23 September 2011