Preventing Wormholes in Multi-hop Wireless Mesh Networks

P Subhash
Department of CSE
Jyothishmathi Institute of Technological Sciences
Karimnagar, A.P, India
subhash.parimalla@gmail.com

S Ramachandram
Department of CSE
University College of Engineering, Osmania University
Hyderabad, A.P, India
schandram@gmail.com

Abstract—Wireless Mesh Networks (WMNs) has become an emerging technology in recent days due to its easy deployment and low setup cost. In WMN, Routing protocols play an important role and these are susceptible to various kinds of internal attacks . One such attack that has severe impact on a WMN is a wormhole attack. A Wormhole is a low-latency link between two parts of the network through which an attacker tunnels network messages from one point to another point. In this paper, we specifically focus on wormhole attack launched by colluding nodes referred to as Byzantine wormhole attack. Unfortunately, most of the existing wormhole defense mechanisms are either centralized, or rely on additional hardware. The major challenge in detecting a byzantine wormhole link is the inability to distinguish nodes involved in the attack process, as they form the legitimate part of network. Being legitimate part of the network, they can bypass all security mechanisms and timing constraints imposed by the network. In this paper, we propose a mechanism to prevent byzantine wormhole attack in WMNs. The proposed mechanism relies on digital signatures and prevents formation of wormholes during route discovery process and it is designed for an on-demand hop-by-hop routing protocol like HWMP (Hybrid Wireless Mesh Protocol-the default routing protocol for WMN). This is simplistic and also applicable to source routing protocols like DSR. This is a software based solution and does not require additional (or) specialized hardware.

Keywords- Wormhole attack; Wireless Mesh Networks; Colluding nodes; Tunnels; Security Mechanisms

I. INTRODUCTION

Wireless mesh networks (WMNs) are gaining more popularity because of its self-healing and self-configuring nature. Potential application scenarios [1] include backhaul support for cellular networks, enterprise networks, community networks, etc. WMN consist of mesh routers and mesh clients, where the mesh routers establish a wireless backbone to provide internet connectivity to the mesh clients. WMN have several advantages such as low-setup cost, increased coverage and also provides flexible and reliable services. Inspite of the above benefits, they are also constrained by the open wireless medium, varying channel conditions and interference. In addition to all the above constraints, meeting security requirements is another challenging task because the open wireless medium is more susceptible to many of attacks. An issues related to various attacks is proposed in [8].

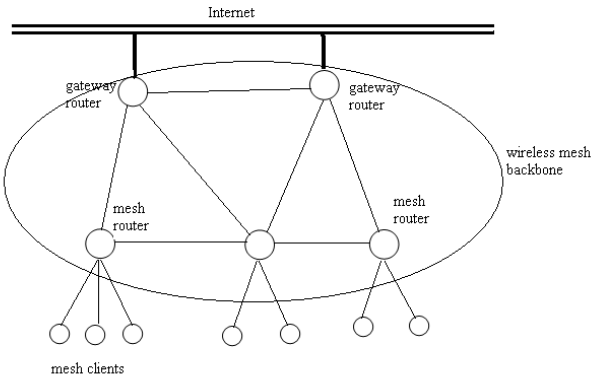

Figure 1: Network Architecture of WMN

Routing protocols in WMN are susceptible to various kinds of internal attacks and one such attack that has severe impact on WMN is a byzantine wormhole attack. Byzantine wormhole attack is a special kind of a wormhole attack, where malicious nodes in the network collude to establish a hypothetical channel between them.This channel can be an out-of-band high-speed communication link or can employ in-band tunneling approach to bypass intermediate nodes. This wormhole link is usually established between two colluding nodes located far away in the network. Once established, the wormhole attracts lot 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 wormhole attack can also be launched even without compromising any node in the network [12]. It is very difficult to detect this kind of attack as the nodes involved in the network activity form legitimate part of the network and just cryptographic mechanisms cannot prevent such kind of attack. But, few unique characteristics exhibited by byzantine wormhole links can enable the nodes sharing the neighborhood with such byzantine nodes to detect and prevent such wormhole links from being established and also isolate such nodes. Essentially, a byzantine wormhole link bypasses several nodes in between to establish a link with a node located at the different part of the network. Thus, a path forming through a byzantine wormhole

978-0-7695-4941-5/13 $26.00 © 2013 IEEE
DOI 10.1109/ACCT.2013.70

advertises a far better metric than any other path in the network. One way to restrict nodes from forming byzantine wormholes is to equip nodes with some mechanism to verify the relative position of nodes. Specifically, it requires nodes to be equipped with GPS systems and a unique way to bind location information with the nodes.

Another alternate way is to check the neighborhood of wormhole links is to determine any abnormal characteristics exhibited by such links. But, it is rather difficult to determine such abnormal links in a network where node s are randomly distributed. As, colluding nodes forming a wormhole link pretend to be genuine neighbors to each other, they cannot be differentiated from a normal to abnormal link without actually confirming the distance between them. Moreover, timing based mechanisms cannot detect byzantine wormholes as the nodes sharing the wormhole are colluded. The other characteristics that can be considered to detect a wormhole link is the large discrepancies in the metric of a path. As path through wormhole link bypasses in between nodes the metric advertised by the wormhole path is much better than any other path, this can be used to detect wormhole links.

II. Related Work

Most of the existing wormhole methods have been designed 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 [2]. It uses two types of packet leashes one is geographic leashes and another one is temporal leashes. But this method requires GPS and tightly synchronized clocks.

Hu and Evans proposed a cooperative protocol [3] in which directional information is shared among nodes to prevent wormhole attack. This method does not required clock synchronization and location information but it requires additional hardware.

Van Tran and Xuan Hung proposed a transmission time based mechanism[4] 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 [5] 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 RREP message with in a stipulated time, it can detect the presence of 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 [6] 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 [7], 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) [10]. 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 abnormal path attraction

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 administered by a Certificate Authority (CA) exists in the network [11]. 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 (Pair-wise 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 processed 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 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 describes the route discovery process. We assume that there exist a path between source and destination which does not consist of any adversaries 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-hop's 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 fig.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 [9] 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 among the set of available paths. Each node receives multiple copies of same PREQ but a node processes only a later received PREQ, if the metric reported by it is better than the previously received metric. But, in order 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 atleast 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 $\{PREQ, NA, S, 1, 0\}_S\{S, 1, 0\}_S$
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 the PREQ with an authenticated message containing ADDR, FLAG, $Metric_I$
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 fig.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	per 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 the Route Discovery Process
2: Broadcast {PPREQ, NA, 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, FLAG, Metric$_I$
12: **end if**

The Proactive PREQ mechanism, the root mesh broadcasts a proactive PREQ element 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 order of the HWMP sequence numbers. Upon receiving a proactive PREQ, a mesh STA 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 transmit 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, a RANN element is periodically propagated by the root mesh STA into the network. Nodes that intend to form a route to the root mesh STA sends an individually addressed 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. 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 thrives on the fact that the path received through a wormhole advertises much better metric than the other paths free of malicious nodes. To enable a network to generate maximum number of versatile paths, nodes transmit all the PREQ's that it receives. 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

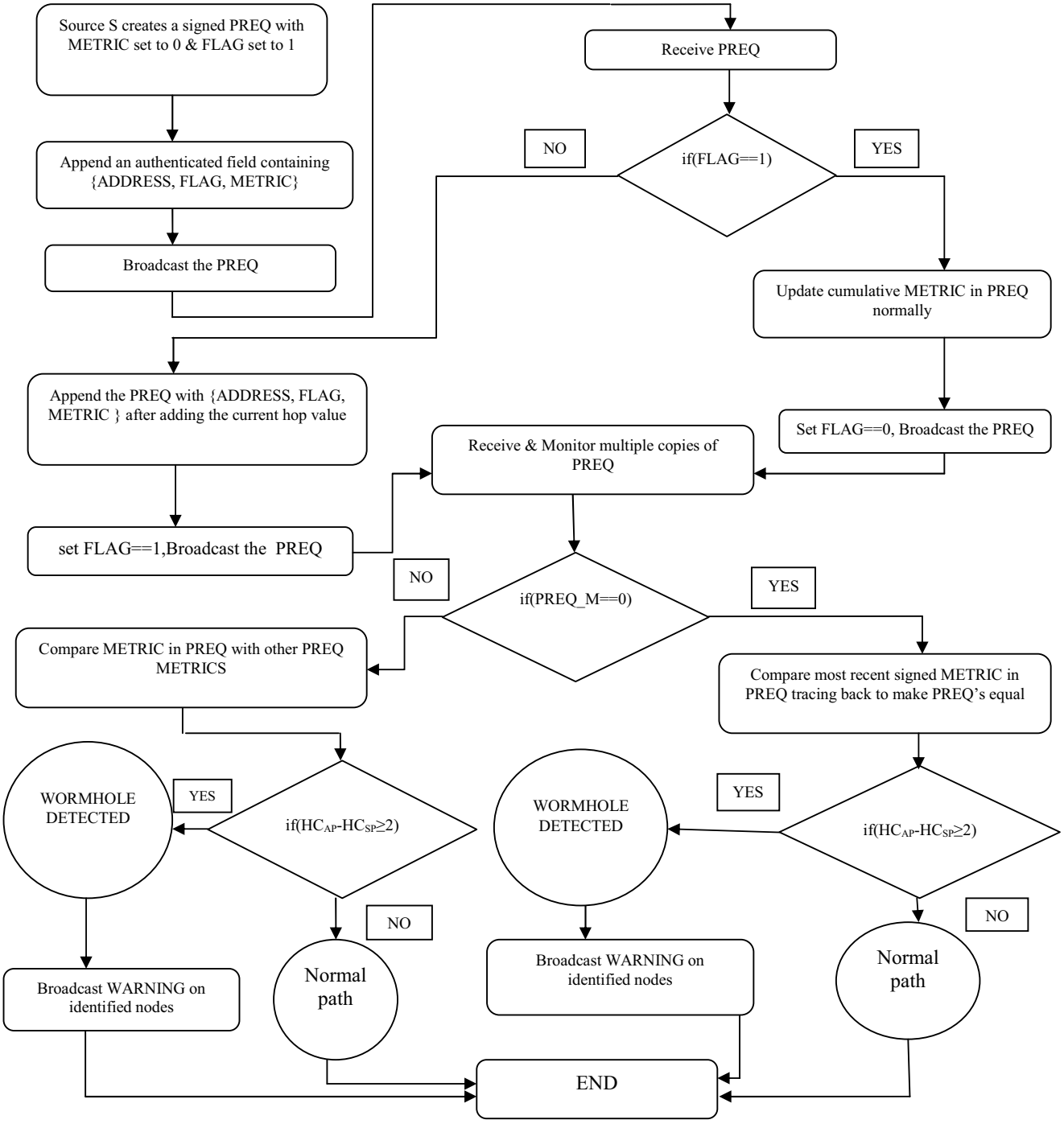

Figure 3: A flow chart of the proposed mechanism

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 neighbor. That effectively limits the capability of a wormhole to a single hop. The intermediate node I that receives 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 mechanism 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 wormhole is greater than ($\geq$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 factious distance of one-hop as claimed by the wormhole, 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 Process
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. 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 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 ($2S_n$) or ($2S_n+1$) hops away from the source.

1) Case(2Sn)

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 alter- nate node to sign the metric field explicitly beginning from the source, in this case the node positioned at the begining of the wormhole link needs to explicitly sign the metric field. Therefore, such node before explicitly signing the metric field, needs to update the cumulate- ive 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 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 atmost 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 lies 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.

1) 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.

2) 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 minimum when a shorter wormhole link is not detected.

VI. CONCLUSION AND FUTURE WORK

In this paper, we presented an efficient mechanism to prevent byzantine wormholes in a WMN. The proposed 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 a 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 increase in the length of a wormhole link. In future this can be evaluated using simulations to compare its performance with the existing protocols.

REFERENCES

[1] Ian F. Akyildiz, Xudong wang, Weilin wang, Wireless mesh networks: A survey,Computer networks and ISDN systems, 2005.

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

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

[4] P. V. Tran, L. X. Hung, Y.-K. Lee, S. Lee, and H. Lee, Ttm: An eficient mechanism to detect wormhole attacks in wireless ad-hoc networks," in In Proc. of IEEE CCNC,2007.

[5] Choi, S., Kim, D.Y., Lee, D.H., and Jung, J.I.: 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.

[6] Hayajneh, T., Krishnamurthy, P., and Tipper, D.: 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, October2009.

[7] Su, M.Y.: 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.

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

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

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

[11] 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 ComputerScience ,Volume 5730,,pp95-114,Springer 2009.

[12] T. Park and K. Shin, “LISP: A Lightweight Security Protocol for Wireless Sensor Networks”, in proceedings of ACM transaction on EmbeddedComputingsystems,August,2004.