Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.413 – 420

RESEARCH ARTICLE

A Study of Manet and Wormhole Attack in Mobile Adhoc Network

Ranjeeta Siwach[1], Vanditaa Kaul[2]
[1]Computer Science & Engineering, BSAITM, Faridabad, M.D University, India
[2]Computer Science & Engineering, BSAITM, Faridabad, M.D University, India

Abstract— Mobile Ad Hoc Networks is the most popular networks widely used in various applications. It consists of mobile nodes where each node communicates with each other. The control of nodes is not administrated by any access point. It generally works by broadcasting the information and used air as medium. Its broadcasting nature and transmission medium also help attacker to disrupt network. Many type of attack can be done on such Mobile Ad Hoc Network.

In this paper, we have analyzed the performance of Mobile Ad-hoc Networks (MANET) under wormhole attack. Wormhole attack makes some malicious node in the network that disrupts to delivery of Packets. This paper provides some important information about wormhole and its detection and prevention methods.

Key Terms: - MANET; wormhole; NEVO

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. They can be set up anywhere without any need for external infrastructure. They are often mobile and that why a term MANET is often used when talking about Mobile Ad hoc Networks. MANETs are often defined as : a" MANET is an autonomous system of mobile routers and associated hosts connected by wireless links- the union of which forms an arbitrary graph. The routers are free to move randomly and unpredictably. Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes . Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The nodes in the network not only acts as hosts but also as routers that route data to/from other nodes in network. It is a collection of mobile nodes, such devices as PDAs, mobile phones, laptops etc., that are connected over a wireless medium. There is no pre-existing communication infrastructure (no access points, no base stations) and the nodes can freely move and self-organize into a network topology. Such a network can contain two or more nodes. Every owner of a mobile phone equipped with a Bluetooth module can build up a direct connection to the other phone and exchange data. It's the simplest form of an ad hoc network, *one hop* piconet. Only one hop is actually not so exciting. Mobile multi-hop ad hoc networks are much more interesting from the point of view of research and application. There are several classes of such networks.

II. WORMHOLE ATTACK IN MANET

An There are two types of wormhole attacks in MANET.

A. Out -of –band wormhole attack:-

Wormhole attacks, in which colluding attackers with out-of-band communication links record packets (or bits) at one location and replay at another, cause far away nodes to consider themselves as neighbors to one another. Such attacks can ruin the routing and communication capabilities of mobile ad hoc networks.

In this attack, an attacker receives packets at one location in the network and tunnels packets to another location in the network, where the packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through a single long-range wireless link or even through a wired link between the two colluding attackers.

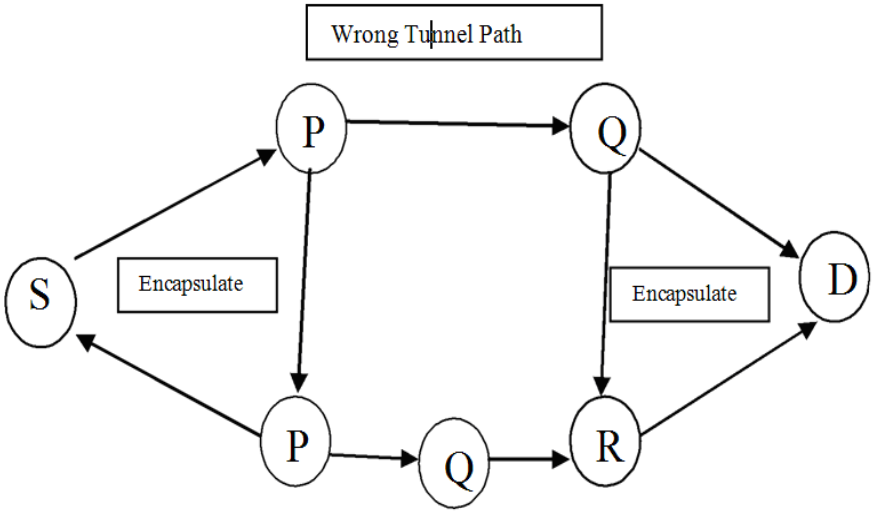

Figure1:wormhole attack in MANET

Due to the broadcast nature of the radio channel, the attacker can create a wormhole even for packets not addressed to itself. **Example:** In figure1. **P** and **Q** are two malicious nodes that encapsulate data packets and falsified the route lengths. Suppose node **S** wishes to form a route to **D** and initiates route discovery. When **P** receives a Route Request from **S, *Q*** encapsulates the Route Request and tunnels it to **Q** through an existing data route, in this case {**P** --> **P** --> **Q** --> **R** --> Q}. When Q receives the encapsulated Route Request for **D** then it will show that it had only traveled {**S** --> **P** --> **Q** --> **D**}. Neither P nor **Q** update the packet header. After route discovery, the destination finds two routes from **S** of unequal length i.e. one is of 4 and another is of 3. If **Q** tunnels the Route Reply back to **P**, **S** would falsely consider the path to **D** via P is better than the path to **D** via R. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of that node. Performance of wormhole attack can be shown in figure 2.In this attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point.

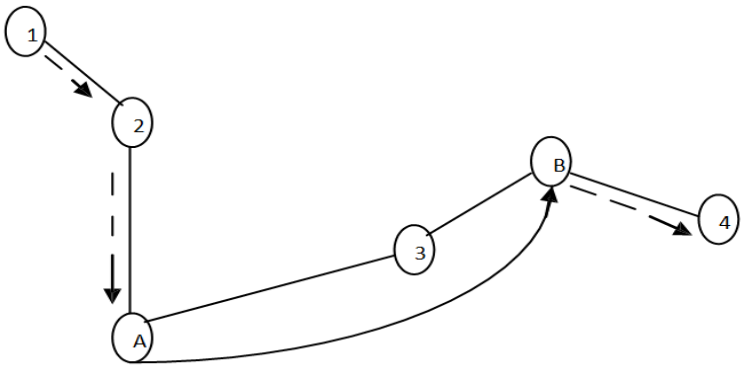

Figure2: A wormhole attack performed by colluding malicious nodes A and B

Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole. Two malicious nodes share a private communication link between them.Worm hole can eavesdrop the traffic, maliciously drop the packets, and perform man-in- the-middle attacks against the network protocols.

B. In-band wormhole attack:- Colluding malicious insider nodes with no special hardware capability can use packet encapsulation and tunnelling to create bogus short-cuts (in-band wormholes) in routing paths and influence data traffic to flow through them. This is a particularly hard attack using which even a handful of malicious nodes can conduct traffic analysis of packets or disrupt connections by dropping packets when needed. Mobile ad hoc networks (MANETs) have a wide range of
applications, especially in military operations and emergency and disaster relief efforts. However, MANETs are more vulnerable to security attacks than conventional wired and wireless networks due to the open wireless medium used, dynamic topology, distributed and cooperative sharing of channels and other resources, and power and computation constraints. Attacker nodes may be insiders – nodes that have the necessary cryptographic keys, participate in normal network operations. We are interested in route falsification attacks caused by insider nodes without special resources such as out-of-band high-speed channels. We show that if an adversary compromises the software of a few insider nodes, then powerful wormhole type attacks can be launched using only the network channels and without requiring physical access to the compromised nodes. In such attacks, colluding insider nodes create bogus short-cuts (wormholes) to routes via existing wireless data paths (in-band channels) and induce other nodes to use these falsified routes. We call these attacks *in-band wormhole attack.*
We use route discovery to learn new routes and route error propagation to remove stale routes. The route discovery consists of two stages.
(1) *Route request stage* – the source node floods the network with a route request control
packet (RREQ), and each intermediate node rebroadcasts the RREQ the first time it hears.
(2) *Route reply stage* – upon receiving a RREQ, the destination sends a route reply packet (RREP), which is propagated to the source in the reverse path
of the RREQ.

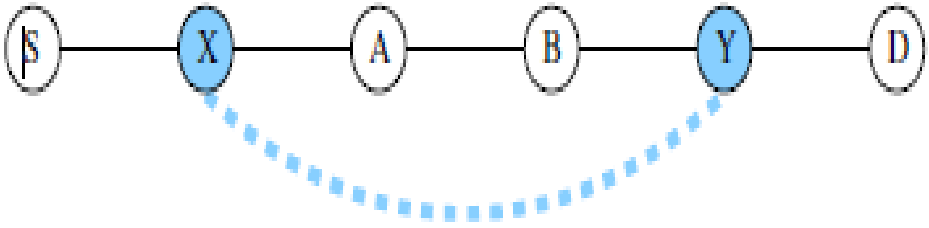

Figure3: Route discovery example. Solid line represents physical wireless link. The dotted line represents in-band wormhole or packet tunnel between X and Y via A and B.

We describe how malicious insider nodes can collude without *a priori* knowledge of the network and using only in-band channels and induce legitimate nodes to use routes through them. Such attacks ensure that there are two or more malicious nodes in a route, one close to the source and another close to the destination. This is desirable for traffic analysis requiring message timing and volume [11]. We use a 5-hop path $S - X - A - B - Y - D$ taken by a RREQ packet from *S* to *D*, Fig. 3, to illustrate these attacks. Nodes *X* and *Y* are colluding malicious nodes and create a packet tunnel between them via normal nodes *A* and *B*. If *Y* obtains the authentication code generated by *X* for RREQ from *S*, then it can fabricate a RREQ which indicates $S - X - Y$ as the path instead of $S - X - A - B - Y$ and send it to *D*. If necessary, the corresponding RREP is tunnelled from *Y* to *X* via *B* and *A*. This results in a false route $S - X - Y - D$ with fewer hops; it cannot be detected even after verification by source/destination. If *S* chooses this bogus path, *X* and *Y* have the option of delivering the data packets or dropping them.

The in-band wormhole attacks are further divided in [2] as 1.1) Self-sufficient wormhole attack, where the attack is limited to the colluding nodes and 1.2) Extended wormhole attack, where the attack is extended beyond the colluding nodes. The colluding nodes attack some of its neighboring nodes and attract all the traffic received by its neighbor to pass through them.
In the second type of wormhole attacks [3], the intrusions are distinguished between a) hidden attack, where the network is unaware of the presence of malicious nodes and b) exposed attack, where the network is aware of the presence of nodes but cannot identify malicious nodes among them.

III. TERMS TO DETECT WORMHOLE ATTACK

There are different types of techniques to detect wormhole attack on network. Mahajn et al. [5] consider several terms for measuring the capacity of nodes involved in wormhole attack. These are defined below:-
1) Strength: - It is amount of traffic attracted by the false link advertised by the colluding nodes.
2) Length: - Larger the difference between the actual path and the advertise path , more anomalies can be observed in the network.
3) Attraction: - This term refers to the decrease in the path length offered by the wormhole. If the attraction is small then the small improvement in normal path may reduce its strength.
4) Robustness:-The robustness of a wormhole refers to the ability of the wormhole to persist without significant decrease in the strength even in the presence of minor topology changes in the network. Besides these, the packet delivery ratio which is the number of packet of delivered divided by the total number of packets dispatched forms a basic metric to quantify the impact.

IV. PREVENTION OF WORMHOLE ATTACK

Choi al et.[6] considered that all the nodes will monitor the behavior of its neighbors. Each node will send RREQ messages to destination. If source does not receive the RREP message within a define time, it detects the presence of wormhole and adds the route to its wormhole list. Each node maintains a neighbor node table which contains a RREQ sequence no. , neighbor node ID, sending time and receiving time of the RREQ and count. The source node sets the Wormhole Prevention Timer (WPT) after sending RREQ packet and wait until it overhears its neighbors retransmission. The maximum amount of time required for a packet to travel one hop distance is WPT/2. Therefore, the delay per hop value must not exceed estimated WPT. However, the proposed method does not fully support DSR as it is based on end-to-end signature authentication of routing packets. Mahajan et al. [5] proposed some proposals to detect wormhole attacks like:
1) The abrupt decrease in the path lengths can be used as a possible symptom of the wormhole attack.
2) With the available advertised path information, if the end-to-end path delay for a path cannot be explained by the sum of hop delays of the hops present on its advertised path, existence of wormhole can be suspected.
3) Some of the paths may not follow the advertised false link, yet they may use some nodes involved in the wormhole attack. This will lead to an increase in hop delay due to wormhole traffic and subsequently an increase in end-to-end delay on the path. An abrupt increase in the end-to-end delay and the hop queuing delay values that cannot be explained by the traffic supposedly flowing through these nodes can lead us to suspect the presence of wormhole. “Time of Flight” is a technique used for prevention of wormhole attacks. It calculates the roundtrip journey time of a message; the acknowledgement estimate the distance between the nodes based on this time, and conclude whether the calculated distance is within the maximum possible communication range. If there is a wormhole attacker involved, packets end up travelling further, and thus cannot be returned within the short time.

V. TECHNIQUES TO MITIGATE IN-BAND WORMHOLE ATTACKS

In this section, we present packet filtering techniques to reject bogus requests and replies that contain in-band wormhole paths. Our techniques are applicable to existing secure routing protocols that require authentication

by each hop during RREQ propagation and end-to-end authentication for RREQs and RREPs. They are based on reducing RREQ delays and statistical profiling of RREQ or RREP delays to prevent creation of in-band wormholes. These techniques may be used by the destination or the source of route discovery.

Reduce requests packet delay

Routing protocols such as AODV [7], DSR [8] and those based on them specify that routing packets should be Propagated at a higher priority than normal data packets. However, that is not enough since malicious nodes can use bogus route reply or route error packets among themselves to exchange attack information speedily. We suggest that, for on demand route discovery schemes that use flooding, requests should be transmitted at a higher priority than all other packets.In order to create an in-band wormhole, two malicious nodes collude and exchange information between each other using data packets (the use of any other packets increases the risk of detection by IDTs). By ensuring that requests travel faster than all other types of packet, we implicitly increase the time to exchange information among malicious nodes.

VI. TECHNIQUE TO MITIGATE OUT-OF- BAND WORMHOLE ATTACK

Causal we propose a network layer based countermeasure in which nodes passively monitor or overhear [9] the forward- ing of certain types of broadcast packets by their neighbors and use the timing information of these broadcast packets to ensure that routes are established through true neighbors only. We call it NEVO (NEighbor Verification by Overhearing). NEVO re- quires broadcasts among neighbors, which are commonly used in ad hoc wireless networks, and local timestamps of broadcast packets sent or received by the medium access control (MAC) layer, which do not require any changes to the MAC protocol but may require a firmware upgrade to enable MAC layer to automatically send this information to the network layer. In contrast to the currently known techniques, NEVO does not rely on special hardware support such as directional anten- nas or ultrasound transimitters/receivers, special capabilities such as clock synchronization or GPS coordinates, geometric inconsistencies, or statistical methods. Therefore, NEVO is a practical solution to mitigate wormhole attacks. NEVO works with all ad hoc network routing protocols. Furthermore, NEVO takes advantage of any broadcasts used by the routing protocol to reduce its overhead.

A. NEVO

We illustrate the approach of NEVO using Fig. 4 in which node i broadcasts a packet, and one of its neighbors, node j, rebroadcasts (forwards) it. We assume half-duplex wireless channels. Let t denote the time it takes a packet to traverse one hop and δ denote the time taken by j to process the packet and acquire the channel before transmitting it. Then, node i overhears j's forwarding in $t + \delta$ seconds after it completed its broadcast if node j is a true neighbor. On the other hand, it takes at least $3t + \delta$ seconds to overhear j's forwarding via a wormhole.

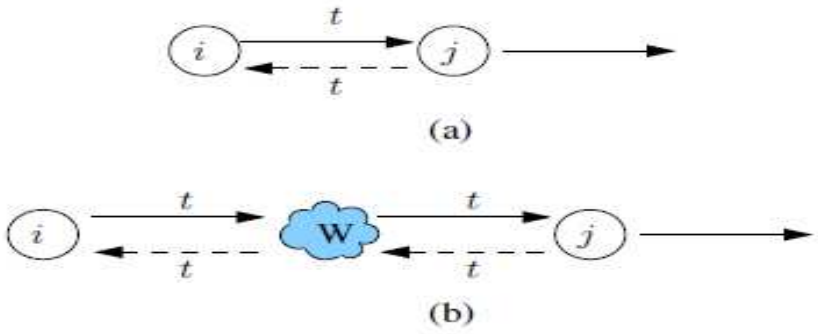

Fig.4. Detection of out-of-band wormholes using passive monitoring. Node i sends a packet to node j and then passively monitors node j's forwarding.
(a) normal case; (b) attack case with a wormhole, W, between node i and node j. W is formed by one or multiple colluding attackers.

B. Timing Analysis of Wormhole Attacks

For a more rigorous timing analysis, we use Figs. 5 (a) and (b) and the following notation.

- t_{s1} (t_{s1}): the local time of node i (node j) at the time the first bit of the message is broadcasted by node i (heard by node j).

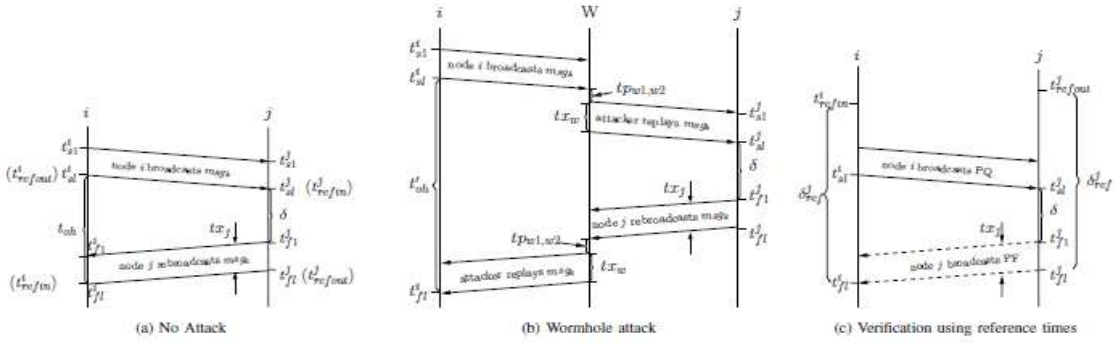

Figure5.Timing Analysis of wormhole attack

- t^i_{sl} (t^j_{sl}): the local time of node *i* (node *j*) at the time the last bit of the message is broadcasted by node *i* (heard by node *j*).
- t^i_{f1} (t^j_{f1}): the local time of node *i* (node *j*) at the time the first bit of the message is overheard by node *i* (forwarded by node *j*).
- t^i_{fl} (t^j_{fl}): the local time of node *i* (node *j*) at the time the last bit of the message is overheard by node *i* (forwarded by node *j*).
- tx_j: the transmission time for the forwarded message by node *j*. It includes preamble and MAC headers. Note that

$t^j_x = t^j_{fl} - t^j_{f1} = t^i_{fl} - t^i_{f1}$.

- δ: the message delay at node *j*, $\delta = t^j_{fl} - t^j_{sl}$
- tx_w: the additional transmission delay incurred to replay the message by a wormhole attacker. This can be as low as one bit time to as much as tx_j.
- $tp_{i,j}$: the message propagation delay between nodes *i* and node *j*.
- t_{oh}: the overhear time, i.e., the time delay for node *i* to overhear node *j*'s forwarding after it broadcasted the message. I.e., $t_{oh} = t^i_{fl} - t^i_{sl}$.
- *R*: maximum radio transmission range in meters.
- S_p: radio signal propagation speed; $S_p < c$, where *c* is the speed of light in free space.

If nodes *i* and ***j*** are true neighbors, see Fig. 5 (a), the propagation delay between them can be estimated as follows.

$t_{oh} = t^i_{fl} - t^i_{sl} = tx_j + \delta + 2tp_{i,j}$ (1)

$t_{oh} - tx_j - \delta = 2tp_{i,j}$ (2)

Note that node *i* knows $tx_j = t^i_{fl} - t^i_{f1}$. In practice, δ, the processing delay at node *j*, varies a lot. However, if node *i* knows δ (suppose, node *j* gave this information in a separate message), then node *i* can verify if the following condition
holds.

$t_{oh} - tx_j - \delta = 2tp_{i,j} \leq 2R/Sp.$ (3)

In the normal case without attack, (3) is satisfied.

In the case of a wormhole link between nodes *i* and *j*, see Fig. 5 (b), the time to overhear, denoted as t'_{oh}, is given by

$t'_{oh} = t^i_{fl} - t^i_{sl} = tx_j + \delta + 2(tx_w + tp_{i,w1} + tp_{w1,w2} + tp_{w2,j})$ (4)

where *w*1 and *w*2 are the two endpoints of the wormhole.

C. Message Transmission Sequence in NEVO

The neighbor verification consists of three message transmissions between two encountered nodes, as shown in Fig. 6 — (1) node *i* broadcasts a control packet, called probe query (PQ) targeted to node ***j***; (2) after node ***j*** receives the PQ from node *i*, it rebroadcasts (forwards) this query packet as its probe forward (PF) packet; then (3) node ***j*** sends node *i* a unicast packet, called probe reply (PR), which contains the processing delay, δ. After receiving PR from node ***j***, node *i* can decide whether to accept node ***j*** as a true neighbor according to (3). To prevent wormhole attackers from fabricating probe packets, nonces are added to PQ and PF packets and a message authentication code to the PR packet. The message formats for PQ, PF, and PR are given as follows:

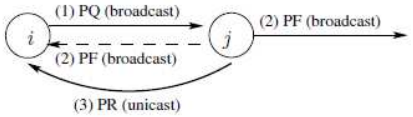

Figure6:Message Transmission Sequence used By NEVO

$PQ_i = \{PQ, i, j, n_i\}$ (5)

$PF_j = \{PF, i, j, n_i, n_j\}$ (6)

$PR_j = \{PR, i, j, n_i, n_j, \delta, M_{ij}\}$ (7)

where n_i and n_j are nonces generated by nodes *i* and *j* respectively, M_{ij} is the message authentication code computed over$\{PR, i, j, n_i, n_j, \delta\}$ using a shared cryptographic key between node *i* and *j*. Note that digital signatures may be used instead of message authentication codes.

Optimization: The broadcast message PF relayed might not be overheard by node *i* due to collision. Even if node *i* receives the PR from node ***j*** but did not overhear ***j***'s forwarding, it cannot decide whether there is a wormhole link between them. Then the neighbor verification fails, and node *i* needs to retry the neighbor verification sequence. To reduce the number of retries, we introduce the concept of reference times. The reference times are local timestamps corresponding to a previous successful event such as the last time nodes *i* and ***j*** verified that they were true neighbors. Consider Fig. 5 (a) in which node *i* initiates the neighbor verification. When node *I* verifies that node *j* is its neighbor, node *i* records t_{isl} and t_{ifl} as the reference times $t_{irefout}$ and t_{irefin}, respectively. Also node *i* sends a special unicast packet to notify node *j* of their true connectivity so that node *j* can record its local timestamps t_{jsl} and t_{jfl} during that verification event as its reference times t_{jrefin} and $t_{jrefout}$, respectively. These reference times are usedfor future neighbor verifications as follows.

We add one more fields to PR, $\delta_{jref} = t_{jfl} - t_{jrefout}$, which is the delay between the time to send the last bit of the PF and the reference time, as shown in Fig. 5 (c). If node *i* receives *a* PR from node *j* and did not overhear the related PF, it can estimate $t_{ifl} = t_{irefin} + \delta_{jref}$ and then verify node *j* according to (3). This works only if nodes *i* and *j* verified each other by overhearing both ways and established the reference times. Node *j* sets $\delta_{jref} = 0$, which indicates that reference time is invalid for neighbor verification, if reference times with node *I* are not established. The reference times $t_{irefout}$ and t_{jrefin} are used for the case where node *j* initiates the verification of node *i*. Potentially, the references times may be updated whenever node *i* verifies node *j* without using δ_{jref}; however, such updates should be done infrequently to reduce the overhead.

VII. CONCLUSION

Wormhole attacks in MANET significantly degrade network performance and threat to network security. The scope of this work is intended to reduce the possibilities of wormhole attacks in an ad hoc network. Wormhole attack in which colluding attackers create a private communication channel(wormhole) between them and replay packets heard at one end of the link to the other end. These wormhole attack can be mitigated by using the technique Reduce request packet delay for In-band wormhole attack and NEVO for Out-of-band wormhole attack**.**

REFERENCES

[1] J.-F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in *Anonymity 2000, LNCS 2009*, 2001, pp. 10–29.

[2] V. Mahajan, M. Natu, A. Sethi. "Analysis of wormhole intrusion attacks in MANETS". In *IEEE Military Communications Conference (MILCOM)*, pp. 1-7, 2008.

[3] H.S. Chiu and K. Lui. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In *Proceedings of International Symposium on Wireless Pervasive Computing*, pp. 6-11, 2006.

[4] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, Nov. 2008 "Analysis of wormhole Intrusion Attacks In MANETS",IEEE Military Communications Conference,MILCOM 2008.

[5] Y.-C. Hu, A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, Security and Privecy Magazine, IEEE, vol. 2, issue 3,pp. 28-39, May 2004.

[6] S.Choi, D.Kim , D. Lee, J. Jung " WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Network ", *In Proceeding International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing*, 2008, pp. 343-348.

[7] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, *Ad Hoc On Demand Distance Vector (AODV) Routing*, IETF, July 2003, RFC 3561.

[8] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (dsr)," in *Internet Draft, draft-ietfmanet-dsr-09.txt*, April 2003.
[9] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of MOBICOM*, pp. 255–265, August 2000.
[10] R. V. Boppana and X. Su, "Secure routing techniques to mitigate insider attacks in wireless ad hoc networks," in *IEEE Wireless Hive Networks Symposium*, 2007

