Location Aware Tunnel Avoidance Wormhole Detection Protocol over MANIT

Akansha Panse[1], Chetan Agrawal[2], Bhavana Verma[3]

[123]*Department of Computer Science & Engineering*

Radharaman Institute of Technology & Science Bhopal, Bhopal

[1]panseakansha1@gmail.com,[2]chetan.agrawal12@gmail.com, [3]bhavanaverma101@gmail.com

Abstract: The wormhole attack is considered a serious threat to the security in multi-hop ad hoc networks. In wormhole attack, the attacker makes the tunnel from one end to another network, the nodes are in a different place at both ends of the tunnel believe are true neighbors and gets the conversation through the wormhole link . Unlike many other ad hoc routing attacks, worm hole attack cannot be prevented by cryptographic solutions because intruders or create new or modify existing packages, but before existing. In this paper a simple technique to effectively detect attacks wormholes without any special hardware and / or location or timing of the stringent requirements proposed. Proposed technique presented an hybrid model that encapsulate route redundancy technique of graphical based scheme and location aided route analysis scheme in order to use advantage of both scheme and increase true positive rate, decrease false negative rate.

Keywords: Wireless Network, Mobile Adhoc Network, Wormhole Attach, LAR Prottocal, Linear Regression,

I. INTRODUCTION

The wormhole attacks pose a serious threat to an ad hoc network for mobile phones. And it cannot easily be registered. A technique has been proposed for detecting the wormhole attacks in MANET. In a wormhole attack, two attack nodes come together. A hacker button receives packets at a given time and "tunnels" to another attack node via a private network connection and then repeats them to the network. The wormhole holds the nodes attacked in a dominant position compared to other nodes on the network in the immediate AODV routing protocols as the attackers in each query packet, route to another attacker close to the node of destiny the tunnel could. When the neighbors on the destination listen to this RREQ, they return this RREQ, and then delete all other RREQs received in the same route search process. This type of attack prevents other routes from being detected instead of the wormhole, thus eliminating a permanent refusal of service attacks for data or specific packages to be removed selectively or a change is required [16].

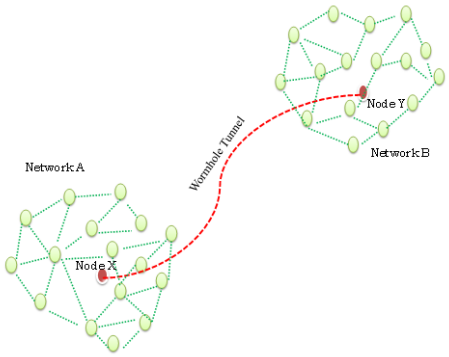
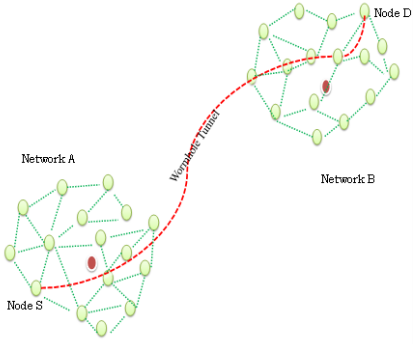


Figure 1: Wormhole attack

II. CLASSIFICATION OF WORMHOLE ATTACKS

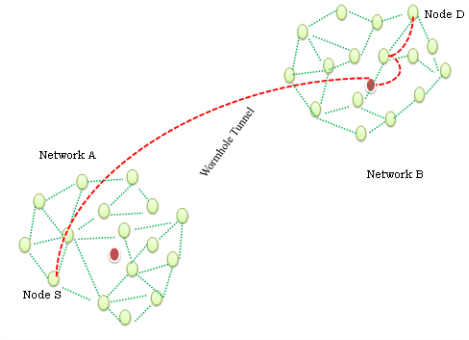
According to whether the assailants are noticeable on the route, wormhole scan be classified into three kinds: open, half-open and closed. The instances that contain two malicious nodes are exposed in Figure 2, consider $M_1$and M_2, and represent the malicious nodes. S and D characterize good knots as source and destination, and A, B, etc. Like good nodes on the route. Buttons between curved brakes ("{}") are buttons on the road, but invisible to Sand D since they are in the wormhole. In the wormhole attack "closed," means, "start from and include," and "open" means, "start from but not include".



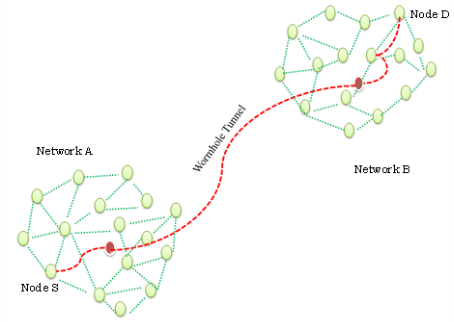
(a)Closed wormhole attack

In (a), M1.and M2.tunnel the neighbor discovery beacons from S to D and vice versa, for this reason S _ and D assume that they are direct neighbors to each other. In Figure(b), M1 is a neighbor of S and it

tunnels its inspirations through M2 to D, Solitary one malevolent node is observable to S _ and D In an vulnerable wormhole, together attackers are evident to S _ and D as shown in (c) [13].



(a) Half open wormhole attack



(b) Open wormhole attack

Figure 2 Classification of wormhole attacks

III. LITERATURE SURVEY

Y. C. Hu et.al [1] present a defense mechanism against network worms: As mobile applications for mobile applications are organized, security is a key requirement. The author presents the pyramid attack. The author presents a new mechanism, called strap bundles, to detect and defend against attacks and wormholes, and to send a specific protocol, called TIK, which implements straps [6].

P. Papadimitratos et.al [2] have discovered a path that reduces adverse effects that lead to bad behavior, to provide adequate link information. The only need for the proposed scheme is the existence of an initiated keyword search and destination safety link. The protocol offers a number of features, such as checking the order to the destination. verifiable return resulting from the response of the request.

K. Sanzgiri et.al [3] have detailed the security threats against ad hoc routing protocols, looking specifically at AODV and DSR. In light of these threats, they identify three different environments with different security requirements and come up with a solution for a managed, open scenario where no network infrastructure has been deployed before.

D. Evans et.al [4] presents an analysis of wormhole attacks and proposes a countermeasure using directional antennas. Its defense greatly reduces the threat of wormhole attacks and does not require location information or clock synchronization [9].

S. Capkun et.al [5] present non-joint assurance verification mechanisms that are sometimes found between nodes in multi-hop wireless networks. The authors proposed SECTOR, a set of protocols for the secure verification of the meeting period between nodes.

R. Maheshwari et.al [6] propose a new algorithm for detecting wormhole attacks in multi-hop wireless networks. The proposed tactic is very localized and, unlike many techniques projected in the literature, does not use material artifacts or slightly exceptional locality information, making the technique universally applicable. The algorithm is independent of wireless communication models.

IV. PROPOSED APPROACH

Proposed technique presented an hybrid model that encapsulate route redundancy technique of graphical based scheme and location aided route analysis scheme in order to use advantage of both scheme and increase true positive rate, decrease false negative rate.

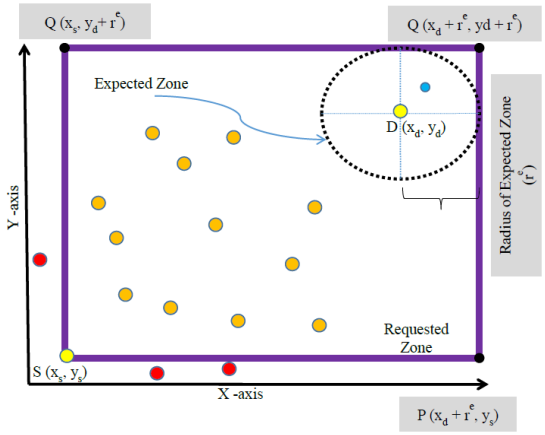


Figure 3 Initial Node

The basic idea of the technique is to discover alternative routes to a target node T which is two-hop neighbor's knots that do not go finished the wormhole. These alternative ways will be lengthily unlike in extent, means the length of another path is superior to the route that have wormhole, and or else the wormhole will not entice large quantities of traffic. Contemplate a collaborating source-destination node pair (S, D), through foundation route $P_{S,\ D}$. If node S want to detect the reality of a wormhole, S would treasure out a new way to T and if

the size of the new route differs extensively compared to the length of $P_{S,T}$ (i.e., superior than a threshold), it is settled that wormhole exists.

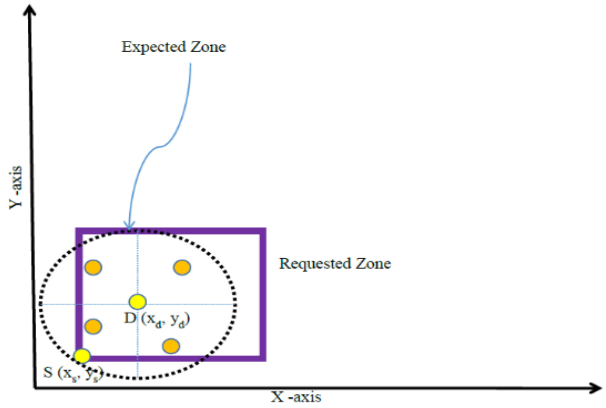


Figure 4: Node Movement

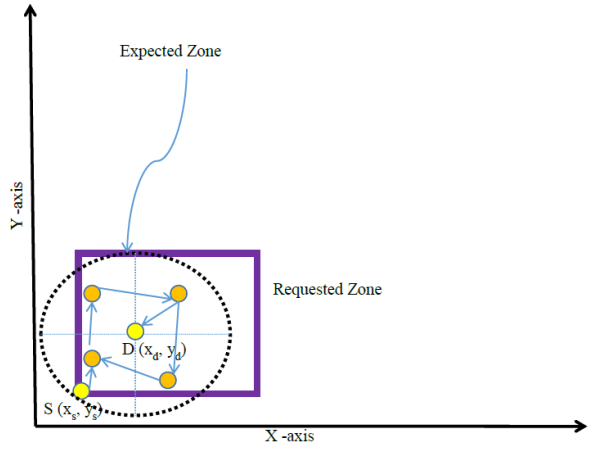


Figure 5: Node Location Changed

I. PROPOSED FRAMEWORK

The proposed framework is shown in figure 6. There are six major component of this framework. Staring with selecting target node where the destination node will decide. In next section hello packet will send to other nodes. After that neighbor node will count. This will help to calculate the number of hopes to get the destination node. This hope count will compare with the threshold which was already calculated. If this hope count will grater then the threshold value so there is wormhole in the network. Otherwise data packet will transfer to the next node.

In the technique for detecting the wormhole in the path, the technique works through the nodes in $P_{S,D}$ (S-source, D-destination) by examining the length of alternate routes between nodes that are a short distance apart. That is alternate path to two hop neighbor on the path starting from S. Consider a source node S that wants to communicate with destination node D and want to test for a wormhole. Let a, b, c belongs to $P_{S,D}$. – they are nodes on the path from S to D that was taken by using some standard routing protocol. Let the wormhole x1 ↔ x2 connect nodes a and b where a belongs to Nx1 and b belongs to Nx2. Let c be the next hop from b on the route from S to D. Note that a and b are typically separated by several hops, but now will believe that they are neighbors.

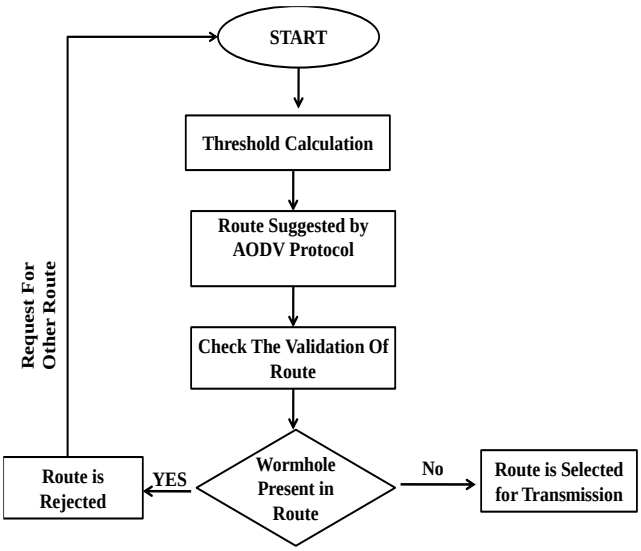


Figure 6 Framework of Algorithm.

The stepwise description of all the process is considered below.

1 In the first step the sender node S will set a target node T that is two nodes away from the sender i.e., $T = P^2_{S,D}$.
2 Sender node S will find all its one-hop neighbors NS by sending a "hello" message. The nodes in NS will listen the hello message and will reply to sender S.
3 Sender build a list of the nodes in NS and pointed node $P^1_{S,D}$.
4 Sender will send the list (NS, T) and request every node r excepted the node from which actual path is made to find a route to T. Each node r will run the network routing algorithm and reply to S with l_{rt} the length (in number of hops) of its route to T. If l_{rt} does not exist then r will inform S and S discards r from the list.
5 S will take an alternate route and find its length. The length of the shortest route is used. The sender tests for the existence of a wormhole by comparing the length of the "selected route" to threshold. If length l_{rt}> threshold then the wormhole is detected.

6 If the no wormhole present, then increment the method to the next hop along the route.
7 In the next step run this process for the entire path from source to destination.

Proposed scheme is based on neighbor node information ie every Ni node find out alternate route for Ni+2 and if minimum of alternate route is greater than threshold proposed scheme generate wormhole presence signal and discard that route .In order to avoid wormhole path proposed scheme suggest AODV find an alternate route between source and destination expect via Ni+1 node. Algorithm for wormhole detection prevention is describing below in algorithm 2.

Threshold is an important part of the proposed technique. In the technique a wormhole tunnel present in the network or not, is decided by the threshold. If the value of alternate path is greater than the threshold, the wormhole is detected. For deciding the threshold considers a network with n number of nodes. In the network, each and every node finds the alternate route to its two hop neighbor that is called target node. The shortest path of minimum number of hop count of each and every alternate path is taken by the algorithm [1]. After that the algorithm consider the highest number of hop count which is comes from these various alternate paths in the whole network and consider highest hop count as a threshold.

Assumption

Ni = Any random node in network somewhere i = 1,2,3,……..n
Nb(Ni)j = Neighbor node of node Ni somewhere j = 1,2,3,…..m
HC(Rx,y) = amount of hop count in route after node x to node y as recommended by AODV
Th(HC) = Threshold hop count
$s^{n}_{(x,y)} = source\ node\ with\ x,y\ co-ordinate$
$d^{n}_{(x,y)} = distination\ node\ with\ x,y\ co-ordinate$
$E(N_{(x,y)}) = energy\ of\ node\ \ N\ with\ x,y\ coordinate$
$V(N_{(x,y)}) = velocity\ of\ node\ N\ with\ x,y\ co\ ordinate$

Algorithms

{
//Expected area covers by destination node

$E^{r} = V(d_{(x,y)}) * (\ t_q - t_p)$ // radius of expected area
$E^{a} = \pi(E^{r})^2$ // Expected area
$M_{(xm,ym)} = \ V(d_{(x,y)}) * (\ t_q - t_p) * tan\,\theta\ \ east$
$E_{(xe,ye)} = \ V(d_{(x,y)}) * (\ t_q - t_p) * tan\,\theta\ \ west$
// Proposed Requested Zone
Proposed requested zone = Area cover by parallel line initialed at point M and L.
// Route $estisbment$
Any random source node(S) request AODV for path concerning their anticipated destination (D)
AODV answer Route reply packet (RRP) with designated path that permit with route R
R = n0, n1, n2,……, nn, nn+1
Someplace
n0 = foundation node
nn+1 = terminus node
ni where i=1 to n is halfway node
For (i = 0 ; i<= n-1 ; i++)
{
For (j = 1 ; j<= m ; j++)
{
Node (ni) refer check location of its neighbour nodule by by means of LAR protocol
and reply (X,Y,Z) organizes

If ([(X1-X)2 + (Y1-Y)2 + (Z1-Z)2]1/2) > radio range)
Formerly
Response wormhole is current in route R
Goto 1
}//end of for loop j
}// end of for loop i
Response route R is designated for transmission
}// algo end

II. RESULT ANALYSIS

The experimentations run over NS2 with 100 nodes scenario and illustration the positive result of worm detection.

- **PACKET DELIVERY RATIO**

Packet delivery ratio is the ratio of the data packets delivered to the destinations to those generated by the traffic sources.

$$PDR = \frac{Number\ of\ data\ packet\ delivered\ to\ distination}{number\ of\ packet\ generated}$$

In any network it is need to increase their packet delivery ratio.
Packet delivery ratio of proposed case i.e. Linear Regression based COTA mechanism for Wormhole Detection and existing case i.e. COTA mechanism for Wormhole Detection has been shown in figure 7 and table 1. As shown in figure Packet delivery ratio of proposed case has been evaluated in scenario of node 100.
As shown in figure during initiation of communication packet delivery ratio of proposed approach has been lag behind existing approach but after certain time performance of LRCOTA is constantly greater than COTA and gradually increase till end. So the performance of LRCOTA is better than COTA.

Table 1: Packet Delivery Ratio

No Of Node	*Number of Delivered Packet*	
	COTA (Existing Approach)	*LRCOTA (Proposed Approach)*
10	87000	96500
20	88500	98670
40	89000	99230
60	86000	95890
80	85500	95230
100	86600	97120

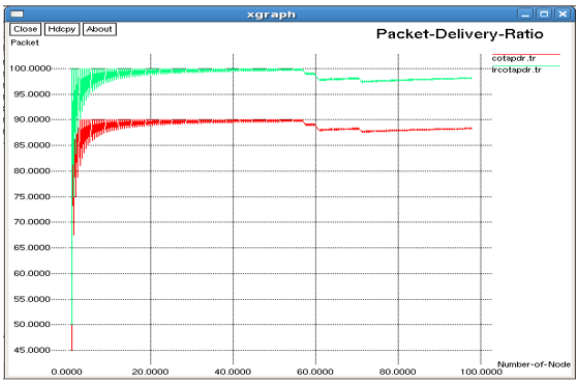


Figure 7 Comparison graph for Packer Delivery Ratio

- **PACKET DELAY**

The latency time that packets used in network must be send from source node to another node. This all happen in the digital data transmission. Sometime the transmission may takes longer time to deliver the packages to their destination, causing an increase in latency, or in other words, delays packets.

$$Packet\ Dela = Total\ Propogation + Total\ Transmmision + Total\ Processing$$

Packet delay of proposed case i.e. Linear Regression based COTA mechanism for Wormhole Detection and existing case i.e. COTA mechanism for Wormhole Detection has been shown in figure 8 and table 2. As shown in figure during initiation of communication packet delay of proposed approach LRCOTA is constantly lower than COTA. So the performance of LRCOTA is better than COTA.

Table 2: Packet Delay

No Of Node	*Number of Packet*	
	COTA (Existing Approach)	*LRCOTA (Proposed Approach)*
10	246	221
20	259	235
40	347	295
60	360	318
80	378	327
100	423	347

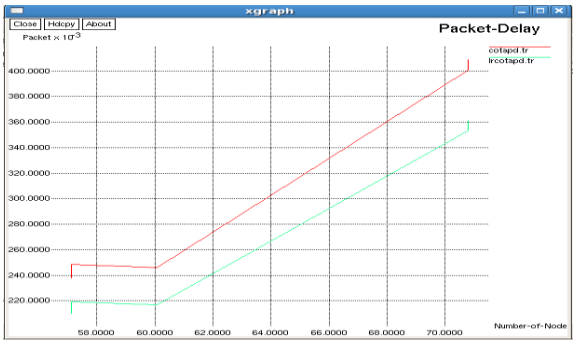


Figure 8 Comparison graph for Packet Delay

- **BATTERY POWER CONSUMPTION**

LRCOTA scheme has two levels node categorization. If mobile nodes of network have maximum M battery power then node with M power should be consider as full power node and node M/4 power should be consider as lower battery power node.

$$Energy\ Consumption = Intial\ energy - Resident\ energy$$

Table 3: Energy Consumption

	Average Energy Consumption Per node	*Energy consumption Over Network*
COTA (Existing Approach)	152 joule	7125 joule
LRCOTA (Proposed Approach)	126 joule	5946 joule

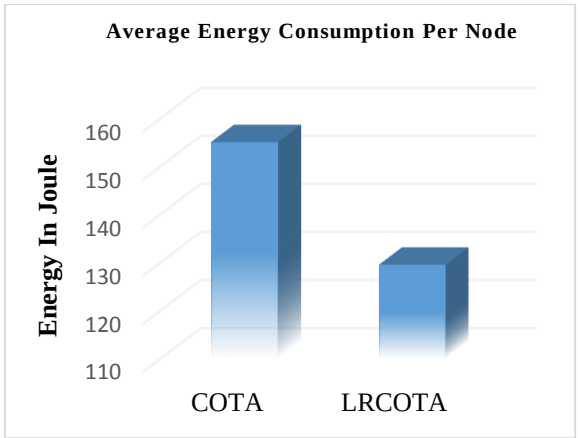


Figure 9 Graph for Average Energy Consumption

If base line node BN(xi,yi) having energy lower than M energy then Base line node call linear regression to find energy efficient node as close as possible.

Towards Energy saving routing protocol proposed protocol tries to choose higher energy node in order to avoid packet drop due to node dehydration and reduce retransmission.

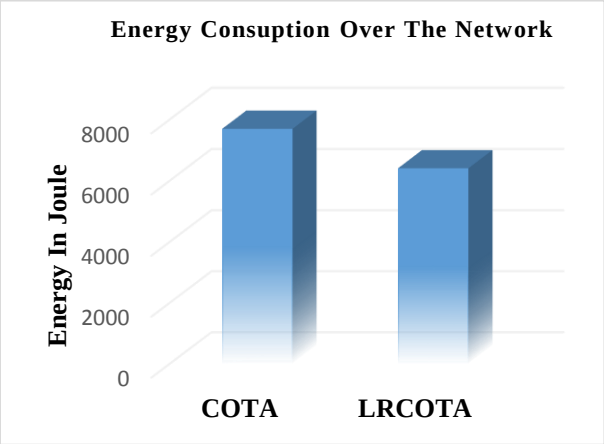


Figure 10 Graph for Total Energy Consumption

As show in figure 9, 10 and table 3 shown average energy consumption of proposed LRCOTA is significantly lower than existing COTA and energy consumption per node is also lower than existing. In case of lower node density scenario COTA have lower energy consumption because in this case energy need to send control packet for battery information lead significant difference. But as network density increase this reflection not gets any significant lead.

- **THROUGHPUT**

The fraction of the channel capacity for effective transmission (packets successfully delivered to the destination data) is given and is defined as the total number of packets received by the destination. It is in effect a measure of the efficiency of a routing protocol. In any sensor network it is required to have higher throughput ie need to increase rate of successful packet transmission.

Table 4: Throughput

No Of Node	***Throughput***	
	COTA (Existing Approach)	*LRCOTA (Proposed Approach)*
10	55.45	65.67
20	60.12	70.23
40	61.23	72.56
60	60.98	71.43
80	56.48	67.79
100	52.46	61.86

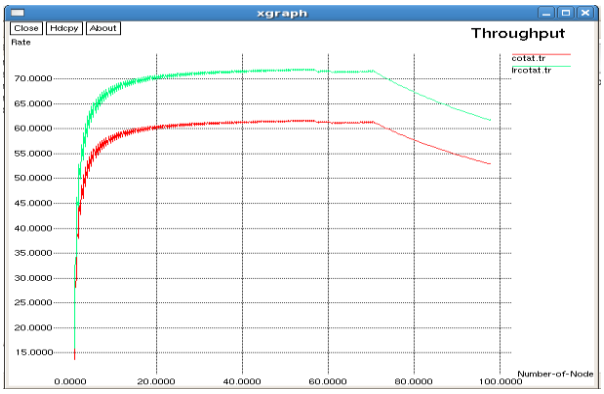


Figure 11 Comparison graph for Throughput

The figure 11 and table 4 shows that detection technology mechanism efficiently, but with a degree of overhead, the control packet also increases in the graph, but the advantage of this technique is that it detects the wormhole and will serve as an advantage once added to the existing AODV protocol be.

III. CONCLUSION

A simple technique for detecting wormholes in ad hoc networks is presented in the paper. This method employs routing variation between neighbors to determine the existence of a wormhole. The technique has been tested through simulations for different distributions of nodes for wormholes and different connectivity models. Besides all the assessed scenarios, the technique demonstrates excellent detection probabilities with few false alarms that depend on the value of threshold. In proposed work degree of False negative rate depend upon value of threshold because of this proposed work not give good result for small network. So in future technique we will develop to overcome this problem. In future a wormhole prevention technique has been proposed that encapsulate proposed wormhole detection technique and minimize overall control packet and routing overhead.

IV. REFERENCES

[1] Y. C. Hu, A. Perrig, and D. B. Johnson, *"Packet leashes: a defense beside wormhole attacks in wireless networks"*, in *Proc. of IEEE INFOCOM*, 2003.

[2] P. Papadimitratos and Z. J. Haas, *"Secure routing for mobile adhoc networks"*, in *Proc. of CNDS*, 2002.

[3] K. Sanzgiri, B. Dahill, E. M. Belding- Royer B. N. Levine, C. Shields, and, "A secure routing protocol of ad hoc networks", in Proc. Of IEEE ICNP, 2002.

[4] Hu and D. Evans, *"Using directional tentacles to prevent wormhole attacks"*, in *Proc. of NDSS*, 2004.
[5] S. Capkun, L. Buttya'n, and J.-P. Hubaux, *"Sector: secure tracking of node meetings in multi-hop wireless networks"*, in *Proc. of the first ACM* workshop on Safekeeping of ad hoc and sensor networks, 2003.
[6] R. Maheshwari, J. Gao, and S. R. Das, *"Detecting wormhole attacks trendy wireless networks exhausting connectivity information"*, in *Proc. of IEEE INFOCOM*, 2007.
[7] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks,"Comput. Netw., vol. 51, no. 13, pp. 3750–3772, 2007.
[8] Y. Lu, and X. Wu, W. Wang, B. Bhargava, "Defending beside wormhole outbreaks in mobile ad hoc networks: Exploration articles,"Wirel. Commun. Mob. Comput., vol. 6, no. 4, pp. 483–503, 2006.
[9] V. Boppana, X. Su and R. "On mitigating in-band wormhole attacks hip mobile ad hoc networks," in Proc. of IEEE ICC, 2007.
[10] Honglong Chena,b, WeiLouc,d, ZhiWang , Jun feng Wue, ZhiboWang , Aihua Xia "Securing DV-Hop localization against wormhole attacks in wireless sensor networks" in Volume 16, Part A, January 2015, Pages 22−35 , Volume 16, Part A, Elsevier 2015, Pages 22−3
[11] K. Jain, J. Padhye, V. N. Padmanabhan and L. Qiu, "Impact of interference on multi-hop wireless network performance," Proc. of the MobiCom, Vol. 11, no. 4, pp 471-487, July 2005.
[12] A. Raniwala, K. Gopalan and T. Chiueh, "Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks," Mobile Computing and Communications Review, vol. 8, no.2, pp. 50–65, April 2004.
[13] M. Alicherry, R. Bhatia and L. Li, "Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks," Proc.ofMobiCom, pp. 58-72, September, 2005.
[14] Soo-Young Shin; Halim, E.H., "Wormhole attacks detection in MANETs using routes redundancy and time-based hop calculation," in ICTC, 2012 International Conference on , vol., no., pp.781-786, 15-17 Oct. 2012