

# AN IMPROVED WORMHOLE ATTACK DETECTION AND PREVENTION IN WIRELESS MESH NETWORKS

T.Vasantha Lakshmi

Nishi Yadav  
Assistant Professor

Deeksha Ekka

Department of Computer Science Engineering  
School of Studies in Engineering and Technology, GGU Bilaspur, India

**Abstract:** Network coding has been shown to be an effective approach to improve the wireless system performance. However, many security issues impede its wide deployment in practice. Besides the well-studied pollution attacks, there is another severe threat, that of wormhole attacks, which undermines the performance gain of network coding. Since the underlying characteristics of network coding systems are distinctly different from traditional wireless networks, the impact of wormhole attacks and countermeasures are generally unknown. In this paper, we quantify wormholes' devastating harmful impact on network coding system performance through experiments. We first propose a centralized algorithm to detect wormholes and show its correctness rigorously. For the distributed wireless network, we propose DAWN, Distributed detection Algorithm against Wormhole in wireless Network coding systems, by exploring the change of the flow directions of the innovative packets caused by wormholes. We rigorously prove that DAWN guarantees a good lower bound of successful detection rate. We perform analysis on the resistance of DAWN against collusion attacks. We find that the robustness depends on the node density in the network, and prove a necessary condition to achieve collusion-resistance. DAWN does not rely on any location information, global synchronization assumptions or special hardware/middleware. It is only based on the local information that can be obtained from regular network coding protocols, and thus the overhead of our algorithms is tolerable. Extensive experimental results have verified the effectiveness and the efficiency of DAWN.

**Keywords:** WMN; Attacks; Security; Routing.

## 1. INTRODUCTION

In the range of discussion the customary worried systems are destroyed because of the remote age. The remote innovation is ease, low upkeep, and quick installable. In this manner various indoor and out of entryways group innovation are progressed to serve steady with the need of administrations. Among some of particular advances the remote work arrangement is one of the imperative innovations. The remote work systems (WMNs) are exceptionally valuable in view of its self-reclamation and self-arranging nature. That can be utilized for versatile portable systems, organization systems, group systems and so on. The WMN is a total switches and clients, where switches set up a remote availability to the customers. WMN have various advantages which incorporate low setup cost, enhanced scope and furthermore displays bendy and trustworthy

administrations [1]. Because of its portable and remote nature the ordinary discussion can be hindered by utilizing the pernicious assailants which incorporates Wormhole, Black-empty, Gray-opening and others. These assaults not just influence the offerings of the group it additionally influence the system general execution of system radically.

## 2. BACKGROUND DETAILS AND RELATED WORK

This section describes the key features of different routing protocols that are supporting the Mobile ad hoc network such as DSDV, OLSR, DSR, and AODV protocols. That also describes the particular parameters that are used for implementing protocols.

### A. Destination-Sequenced Distance Vector (DSDV)

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. The improvement made to the Bellman-Ford algorithm includes freedom from loops in routing tables by using sequence numbers. It was developed by C. Perkins and P. Bhagwat in 1994. The DSDV protocol can be used in mobile ad hoc networking environments by assuming that each participating node acts as a router. Each node must maintain a table that consists of all the possible destinations. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle. Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges; thus, DSDV is not suitable for highly dynamic networks [2].

### B. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks and is based on a method known as source routing. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. Except that each intermediate node that broadcasts a route request packet adds its own address identifier to a list carried in the packet. The destination node generates a route reply message that includes the list of addresses received in the route request and transmits it back along this path to the source. Route maintenance in DSR is accomplished through the confirmations that nodes generate when they can verify that the next node successfully received a packet. These confirmations can be link-layer acknowledgements, passive acknowledgements or network-layer acknowledgements specified by the DSR protocol. However, it uses source routing instead of relying on the routing table at each intermediate device. When a node is not able to verify the successful reception of a packet it tries to retransmit it. When a finite number of retransmissions fail, the node generates route error message that specifies the problematic link, transmitting it to the source node [3].

### C. Ad-hoc on Demand Distance Vector (AODV)

AODV is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV [4]. In order to maintain routes, AODV normally requires that each node periodically transmit a HELLO message, with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbour is taken as an indication that the link to the neighbour in question is down. Alternatively, the AODV specification briefly suggests that a node may use physical layer or link layer methods to detect link breakages to nodes that it considers neighbours [4].

### D. Wormhole attack

Wormhole assault is a particular type of inner assault, wherein malevolent nodes within the network plan to establish an imaginary channel between them. This channel can be an out-of-band excessive-speed verbal exchange hyperlink or can hire in-band tunneling approach to bypass intermediate nodes. This wormhole hyperlink is typically mounted between two colluding nodes located a long way away inside the network. Once diagnosed, the wormhole captures a variety of site visitors because it advertises a whole lot higher hyperlink metric than some other paths in the network. The wormhole nodes can then initiate diverse sorts of denial of carrier (DoS) assaults that strictly affect the habitual of the network. It is very tough to locate this form of assault as the nodes worried within the network action form genuine part of the network and simply cryptographic mechanisms can't prevent such kind of assault .[10]

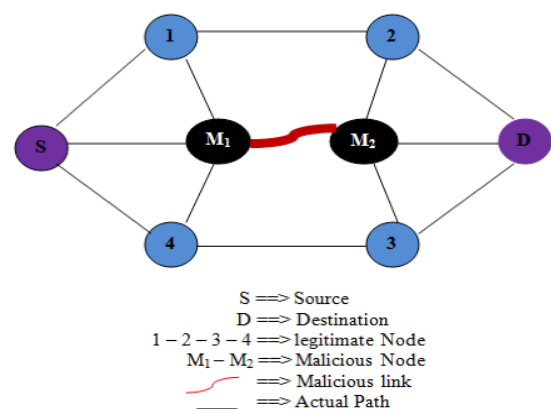


Fig-1:Wormhole Attack.

### 3.LITERATURE SURVEY

#### E. Packet Leashes

The main scheme is that by authenticating either an extremely accurate timestamp or place information joint with a slack timestamp, a receiver can decide if the packet has traversed an impractical distance for the definite network technology used. Packet leashing was added to each packet on each link to confine the transmission distance of the packet. Two types of packet leashes could be added into the packet. One is geographical leash in which the sender put up its own position and sending time into the packet, the receiver will compute the maximum distance between the sender and itself based on its own position and receiving time. If the distance exceeds the transmission range, the packet will be discarded. The other type is temporal leash. This mechanism assumes that the utmost transmission hustle of radio signal is the speed of light, thus the ending time of a packet can be estimated using the maximum transmission range and the speed of light. The ending time of the packet is inserted into the packet, and then the receiver can ensure whether the received packet has expired or not based on its receiving time. A disadvantage of packet leashes is that it requires extremely tight time synchronization and GPS [5].

#### F. TTM

Van Tran and Xuan Hung proposed a transmission time based mechanism (TTM) for detecting wormhole attacks. This method calculates each Round Trip Time (RTT) between two consecutive nodes along the route. Each node in the path will estimate RTT between it and the destination, this value will be sent back to the source. A wormhole will be recognized based on the detail that transmission time between two wormhole nodes is considerably larger than that between two genuine consecutive nodes. Although Time based protocols have advantages of providing ease of use, low division overhead and the high efficiency of the proposed mechanism. But still they need some approximations as the node that is in charge of detection has to account for the processing and propagation delay times. More significantly, these protocols are unable to detecting out- of-band physical layer wormholes because a packet suffers only the propagation delay which could be limited by for wormholes using high-speed links [6].

#### G. Directional Antenna

Hu and Evans suggested a solution via a supportive protocol in which directional information is pooled among nodes to avoid wormhole attack. In this, which all nodes are equipped with directional antennas where nodes uses precise „sectors“ of their antennas are communicate to each other. Each pair of nodes has to examine the direction of received signals from its neighbour. Therefore, the neighbour relation is confirming only if the directions of both pairs match. This process does not required clock synchronization and position information but it requires extra hardware [7].

#### H. Sector

Capkun et al. introduce a new method which also needs a specialized hardware and utilize end to end packet leashes. The method takes into account the speed of the transmission among the two nodes. They presented a new protocol named “SECure Tracking Of Node EncounteRs in Multi-hop Wireless Networks” i.e. SECTOR, although it doesn't need any clock synchronization and position information, by using Mutual Authentication with Distance-Bounding (MADB), though it needs accurate calculation of the distance and needs GPS coordinates of all node. MADB Protocol is used for distance estimation. Node X can estimate the distance to a node Y based on the speed of data transmitted between them. Every node uses a particular hardware that enables quick sending of one-bit challenge messages without CPU participation to reduce all possible processing delays. By using the time of flight, X identify whether or not Y is a neighbour. This technique is partial by the limitations of the GPS technology [8].

#### I. Graph Theoretical Based Approach

Lazos and Poovendran proposed Localization based method a “graph theoretical” approach to wormhole attack prevention. The whole procedure is based on the use of limited location-aware guard nodes (LAGNs) which are in the well-known location and initiation and achieved through GPS receivers. LAGNs use "local broadcast keys" that are legitimate only between direct one hop neighbours. In order to sense wormhole attack, it is not possible to decrypt a message encrypted with a local key – encrypted with the pair-wise key. Thus during the key generation, method used hashed messages from



LAGNs to detect wormholes. A node can detect definite inconsistencies in messages from different LAGNs if a wormhole is present. In the absence of wormhole, a node is unable to have the sense of hearing two LAGNs that are away, and are not able to hear the similar message from one guard double [9].

### J. *Digital Signature Approach*

In this mechanism, a key based method for preventing wormhole attack in wireless mesh network, planned method relies on digital signature and averts structure of Wormholes throughout route detection procedure and it is intended for an on command hop-by-hop routing procedure. Here not requires additional or specialized hardware [10].

### K. *Delphi*

To avoid the need of synchronized clocks, positioning device and other special hardware Chiu et al. proposed a new technique is DELPHI i.e. DELay Per Hop Indicator that uses delay as a parameter. The detection method uses the delay/hop value for detecting wormhole attacks. In this Delphi collects information and perform detection at sender and obtain delay and hop count information. When the detection is initiated, the sender broadcast a request message to the receiver, and receiver replies all the request messages received. In this way sender can obtain the information of some disjoint paths to the receiver. By comparing the Delay/Hop values among these disjoint paths, a wormhole can be identified. This method has two phases: (1). Delay and hop count information is collected, (2). the sender analysis the information obtain in the first phase to detect there is any wormhole attack [11].

### L. *WAP*

Choi and Kim presented Wormhole Attack Prevention algorithm (WAP) is a neighbour monitoring based method. All the nodes will observe its neighbour's behavior when they send RREQ messages to the destination with the assist of neighbour list. If the source does not get RREP message with in a wormhole prevention timer (WPT), it can sense 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 with no

requiring special hardware. This scheme does not fully support DSR because it is based on end-to-end signature verification of routing packets [12].

### M. *LITEWORP*

Khalil et al presented LiteWorp, which assumes the existence of an attack-free environment before the wormhole attacks are launched, a lightweight protocol called LITEWORP to detect these malicious nodes and remove the wormhole attacks in Ad-Hoc networks. This proposed protocol uses secure two hop neighbour discovery and information about the whole traffic to detect the malicious nodes which are part of the wormhole attack. In LITEWORP, they can take advantage of two-hop, rather than one-hop. This information can be exploited to detect wormhole attacks. These nodes also observe their neighbours' behavior to determine whether data packets are being properly forwarded by the neighbour. This technique isolates the malicious nodes and provides the secure network for future routing [13].

### N. *MDS-VOW*

Wang et al. proposed a Multi-Dimensional Scaling-Visualization of Wormhole (MDS-VOW) procedure which used to detection of wormhole attack in wireless network. In this scheme using the received signal strength, each node measures the distance to its neighbour. Based on these measurements, base station computes the physical topology of the network. It is observed that the network with malevolent nodes has diverse visualization from that with usual nodes. In absence of wormholes, topology should be more or less flat, where as in their occurrence „string“ pulling different ends of network are seen. It recreates the layout of the sensors using multidimensional scaling scheme. The anomalies, which are introduced by the false connections through the wormhole, will turn the reconstructed surface to pull the sensors that are far away to each other. Therefore, MDSVOW could place the wormhole connections. In MDSVOW, all sensor nodes are necessary to send their neighbour lists to the base station [14].

## 4. PROPOSED ARCHITECTURE

In this section, the idea to detect wormhole attack is presented based on the knowledge gathered on the survey. In the review papers various techniques

have been adopted to detect the wormhole attack. In my proposed work there is a centralized and distributed algorithm to detect wormhole. Here we define a threshold value for data transfer. We consider a public key infrastructure for implementing the public key infrastructure. In wireless network we consider each node as a user that has a pair of private and public keys. There is a central authority (CA) in the infrastructure which maintains the identity information of each user. It is a trusted entity which is also responsible for pre-distributing and revoking the key. During the data transfer the sender will request the receiver public key for encrypting the data and the receiver will request the sender public key from CA for decrypting the data. Here when the data transfer takes place the centralized node will monitor whether any innovative packets arrives to a node within the communication range. Each node has a rank and time stamp value. If innovative packets arrive then the rank of each node will be incremented. Next the centralized algorithm will calculate the expected transmission count (ETX) that describes the expected total number of transmission to complete the data transfer. If the ETX value exceeds the threshold value then the centralized algorithm will find the wormhole links. In case if there is no central node to monitor the nodes, then the distributed algorithm takes place. Here the entire network is divided into the cluster. The cluster head will be chosen from each cluster and then assign the role to monitor the nodes. The distributed algorithm will takes place in absence of centralized node. Thus the centralized and distributed algorithm provides a greater contribution in detecting the wormhole attack. The overall architecture is presented below, where the centralized algorithm technique is implemented to detect the wormhole attack.

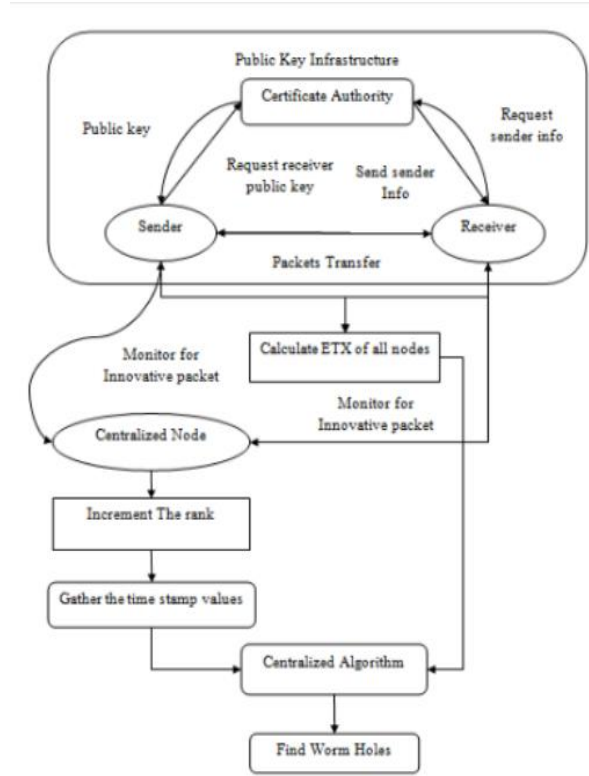


Fig-2:Architecture.

## 5.IMPLEMENTATION

### O. Algorithm to Determine ETX

**Input:** the entire network  $G$  with nodes  $V$  and their locations  $L$ , and the source node  $v_s$   
**Output:** the ETXs for all the nodes in the network  $G$

- 1:  $ETX(v_s) \leftarrow 1.0$
- 2: **for** each node  $v_i$  in  $V$ , except  $v_s$  **do**
- 3:      $ETX(v_i) \leftarrow +\infty$
- 4: **end for**
- 5: **repeat**
- 6:      $ETX_{updated} \leftarrow false$
- 7:     **for** each node  $v_i$  in the network  $G$ , other than  $v_s$  **do**
- 8:         Let  $N$  be the set of the neighbors of  $v_i$  s.t.  $ETX(v_k) < +\infty$  for any  $v_k \in N$
- 9:         **if**  $ETX(v_i) > \frac{1}{1 - \prod_{v_k \in N} \frac{1}{ETX(v_k)} (1 - P(v_k, v_i))}$  **then**
- 10:              $ETX(v_i) \leftarrow \frac{1}{1 - \prod_{v_k \in N} \frac{1}{ETX(v_k)} (1 - P(v_k, v_i))}$
- 11:              $ETX_{updated} \leftarrow true$
- 12:         **end if**
- 13:     **end for**
- 14: **until**  $ETX_{updated} = false$
- 15: **return** the ETXs for all the nodes

### P. The Centralised Algorithm

In this section, we propose the centralized algorithm, which utilizes the ETX metric and the order of rank increment to detect wormhole attacks. In order to protect the validity of our method, we also introduce the public cryptographic scheme for the network. For the proposed algorithm, we not only perform the analysis of its correctness, but also discuss its technical details in this section.

**Simulation Scenario**

In order to perform the experiments the following one-of-a-kind scenarios are prepared for simulation and community overall performance opinions.

1. Simulation underneath AODV Routing Protocol with Wormhole Attack: on this community simulation the network is configured with AODV routing protocol and the network performance is evaluated. That simulation additionally incorporates a malicious wormhole hyperlink which demonstrates the results of wormhole attack in ordinary community.

AdversaryNode				
Packet Count	Packet Length...	Bandwidth(Kbs...	TimeDelay(ms)	Packet Status
28	1000.0	0.099609375	0.102	Pure Packet Al...
27	1000.0	0.09765625	0.1	Pure Packet Al...
26	1000.0	4.883789	5.001	Wormhole Att...
25	1000.0	4.8828125	5.0	Wormhole Att...
24	1000.0	4.8828125	5.0	Wormhole Att...
23	1000.0	4.883789	5.001	Wormhole Att...
22	1000.0	4.883789	5.001	Wormhole Att...
21	1000.0	4.883789	5.001	Wormhole Att...
20	1000.0	4.8847696	5.002	Wormhole Att...
19	1000.0	0.10098994	0.103	Pure Packet Al...
18	1000.0	4.883789	5.001	Wormhole Att...
17	1000.0	4.8828125	5.0	Wormhole Att...
16	1000.0	4.8828125	5.0	Wormhole Att...
15	1000.0	4.8828125	5.0	Wormhole Att...
14	1000.0	4.8828125	5.0	Wormhole Att...
13	1000.0	0.09863281	0.101	Pure Packet Al...
12	1000.0	0.099609375	0.102	Pure Packet Al...
11	1000.0	4.883789	5.001	Wormhole Att...
10	1000.0	0.09863281	0.101	Pure Packet Al...
9	1000.0	0.099609375	0.103	Pure Packet Al...
8	1000.0	4.8828125	5.0	Wormhole Att...
7	1000.0	0.09863281	0.101	Pure Packet Al...
6	1000.0	4.883789	5.001	Wormhole Att...
5	1000.0	4.883789	5.001	Wormhole Att...

Fig-3:Network under Attack

2. Simulation for Proposed Method under AODV Routing Protocol with Attack Prevention: n this simulation the proposed comfortable routing protocol is applied in the community simulator 2 with the same configuration as the alternative networks is configured. After that for investigating the impact of the proposed answer the wormhole link is applied on the community and the network performance is predicted via end result evaluation.

AdversaryNode				
Packet Count	Packet Length...	Bandwidth(Kbs...	TimeDelay...	Packet Status
96	1000.0	4.883789	5.001	Wormhole Attack ...
95	1000.0	4.883789	5.001	Wormhole Attack ...
94	1000.0	4.8828125	5.0	Wormhole Attack ...
93	1000.0	4.883789	5.001	Wormhole Attack ...
92	1000.0	4.883789	5.001	Wormhole Attack ...
91	1000.0	4.8828125	5.0	Wormhole Attack ...
90	1000.0	4.883789	5.001	Wormhole Attack ...
89	1000.0	0.10098994	0.103	Pure Packet Allo...
88	1000.0	4.8828125	5.0	Wormhole Attack ...
87	1000.0	4.883789	5.001	Wormhole Attack ...
86	1000.0	4.883789	5.001	Wormhole Attack ...
85	1000.0	4.883789	5.001	Wormhole Attack ...
84	1000.0	4.883789	5.001	Wormhole Attack ...
83	1000.0	4.883789	5.001	Wormhole Attack ...
82	1000.0	0.09863281	0.101	Pure Packet Allo...
81	1000.0	4.8828125	5.0	Wormhole Attack ...
80	1000.0	4.8828125	5.0	Wormhole Attack ...
79	1000.0	4.883789	5.001	Wormhole Attack ...
78	1000.0	4.883789	5.001	Wormhole Attack ...
77	1000.0	4.883789	5.001	Wormhole Attack ...
76	1000.0	4.8828125	5.0	Wormhole Attack ...
75	1000.0	4.883789	5.001	Wormhole Attack ...
74	1000.0	4.8828125	5.0	Wormhole Attack ...
73	1000.0	4.8828125	5.0	Wormhole Attack ...

Fig-4:Proposed method

**6. RESULTS AND ANALYSIS**

Graphs are plotted and concluded that proposed scheme has improve throughput value and packet shipping ratio also reduces end to stop routing put off.

**Q. End to quit put off**

End to give up delay on network refers to the time taken for a packet to be transmitted throughout a network from supply to vacation spot tool.

Mixnetwork			
Packet Count	Packet Length(Bits)	Bandwidth(KBs/ps)	TimeDelay(ms)
107	1000.0	0.09765625	0.1
106	1000.0	0.09765625	0.1
105	1000.0	0.09765625	0.1
104	1000.0	0.09765625	0.1
103	1000.0	0.09765625	0.1
102	1000.0	0.09765625	0.1
101	1000.0	0.09863281	0.101
100	1000.0	0.09765625	0.1
99	1000.0	0.09765625	0.1
98	1000.0	0.09863281	0.101
97	1000.0	0.09863281	0.101

```

Received File
%PDF-1.4
%âãÏ
1 0 obj
<</Metadata 2 0 R/Outlines 5 0 R/Pages 3 0 R/SaveStreams<</Q 6 0 R/q 7 0 R>>/Type/Ca
endobj
2 0 obj
<</Length 3746/Subtype/XML/Type/Metadata>>stream
<?xmlpacket begin="ï¿½" id="W3M0MtpCehiHzeRSnTczk9d"?>
    
```

Fig-5: End-to-End Delays Cease to quit delay in phrases of milliseconds. The overall performance of the proposed approach is simulated thru inexperienced line.

**R. Packet Delivery Ratio**

Packet transport ratio gives facts about the performance of any routing protocols, where PDR is expected the usage of the system given Packet Delivery Ratio = Total Received Packets to Total Sent Packets. In this diagram the X-axis indicates the simulation time of the community and the Y-axis indicates the packet shipping ratio in phrases of percent.

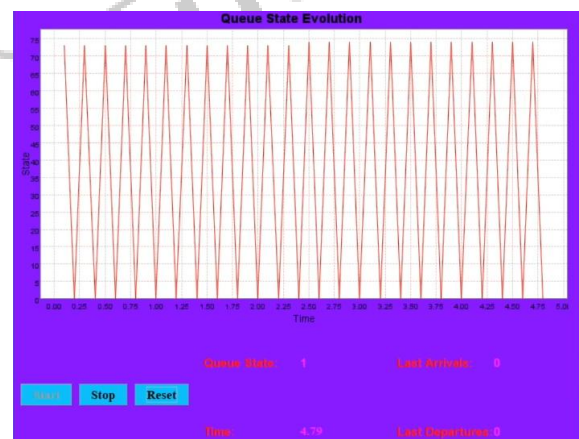


Fig-6:Packet Delivery Ratio

**7.CONCLUSION AND FUTURE WORK**

Remote work systems are at risk to extensive variety of insurance assaults because of their arrangement in an open and unprotected environment. This examinations work explores



special wormhole recognition methodologies, looks at different existing techniques to find how they were done to unearth wormhole ambushes. Every method has its own special quality and shortcomings. We offered a proficient system to spare you Wormholes on WMN. The proposed instrument is shortsighted and does not depend on additional like GPS frameworks. The execution of the proposed strategy is given the utilization of the java environment. For general execution examination is executed utilizing the produced arrange follows. The general execution of the actualized steering approach is imagined as far as parcel conveyance proportion, throughput, and quit to end delay.

### Future Work

The proposed approach can be reached out by the utilization of various situations in systems.

1. The given strategy is a parameter essentially based method which uses the system parameters for finding the vindictive connection subsequently that approach can be drawn out for actualizing security for various assaults basically in view of the system parameter choice.
2. The Future Scheme of the whole research is to expand the proposed plan to various conventions instead of the AODV convention. The system is intense and productive at some phase in strike conditions subsequently the method is utilized for likewise to improve the system security in different remote advert hoc systems comprehensive of VANET, WSN and others.

### 8. REFERENCES

1. IAN F. AKYILDIZ, XUDONG WANG, "A Survey on Wireless Mesh Networks", IEEE Radio Communications, September 2005, 0163-6804/05/\$20.00 © 2005 IEEE
2. S. A. Ade and P. A. Tijare, "Execution Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 545-548, July-December 2010
3. Nikhil Kumar, Vishant Kumar and Nitin Kumar, "Close Study of Reactive Routing Protocols AODV and DSR for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies (IJCSIT), Volume five, pp.6888-6891, 2014.
4. M. S. Karthikeyan, K. Angayarkanni, and Dr. S. Sujatha, "Throughput Enhancement in Scalable MANETs the use of Proactive and Reactive Routing Protocols", In Proceedings of the International Multi Conference of building and programming designing, Volume 2, March 2010.
5. Hu, Y. Perrig, An., and Johnson D., Packet Leashes: "A Defense against Wormhole Attacks in Wireless Network", In Proceedings of the twenty second IEEE International Conference Computer and Communications, Volume three, pp.1976– 1986, April 2003.
6. P. V. Tran, L. X. Hung, Y. Lee, S. Lee, and H. Lee, TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-Hoc Networks, In Proceeding of fourth IEEE CCNC, pp. 593-598, Las Vegas, USA, Jan. 2007.
7. L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," In Network and Distributed System Security Symposium (NDSS), San Diego California, USA, five-6 February, 2004.
8. S. Capkun, L. Buttyan and J.P., Hubaux, "Part: Secure Tracking of Node Encounters in Multi-hop Wireless Networks", In Proceedings of first ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS), pp. 21-32, New York, USA, 2003.
9. L. Lazos and R. Poovendran, "Serloc: Secure collection fair control for Wireless Sensor Networks", In Proceedings of the ACM Workshop on Wireless Security, pp. 21–30, October 2004.
10. P Subhash and S Ramachandram, "Maintaining a strategic distance from Wormholes in Multihop Wireless Mesh Networks", Third International Conference on Advanced Computing and Communication Technologies, pp. 293-three hundred, 2013.
11. H.S. Chiu and K.S. Lui, "DELPHI: Wormhole Discovery Device for Ad-hoc Wireless Network", first International Symposium on Wireless Pervasive Computing, pp. 6– 11, Phuket, Thailand, sixteen-18 January 2006.
12. C. Sun, K. Doo-more young, L. Do-hyeon and J. Jae-il, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," In Proceeding of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), pp. 343-348, 2008.
13. Khalil S. Bagchi and N.B. Shroff. LITEWORP: A Lightweight Countermeasure for the

Wormhole Attack in Multi-hop Wireless Networks, International Conference on Dependable Systems and Networks, pp.612–621, 2005.

14. W. Wang and B. Bhargava, "Portrayal of wormholes in sensor frameworks", In Proceedings of the third ACM workshop on Wireless security, October 01, Philadelphia, PA, USA, 2004.

