International Journal of Future Generation Communication and Networking
Vol. 9, No. 6 (2016), pp. 41-54
http://dx.doi.org/10.14257/ijfgcn.2016.9.6.05

Trust and Reputation Based Seurity of MANET by Worm Hole Attack

Shabina Parbin[1] and Leeladhar Mahor (*Asst. Prof*)[2]

Dept. of CSE[1, 2]
NITM Gwalior, India[1, 2]
shabina.sheikh22@gmail.com[1] and ldmahor@gmail.com[2]

Abstract

Mobile ad-hoc network is one of the most attractive fields for research. Any new node easily entered or left the network because of this property is easily thretend by the attack. A wormhole is one of the most crucial attack of MANET in this paper, we study lots of prevention and detection technique. In our propose work we work on trust and reputation mechanism and then secure network novelity of proposed work we proof by our outcomes.

Keywords*: MNET;AODV;RREQ;RREP*

1. Introduction

Mobile wireless ad hoc networks (MANETs) are basically specific from wired networks, as they use wireless medium to communicate, don't depend on constant infrastructure, and may arrange them into a network rapidly and quite simply. In a MANET, each and every node serves as a router for distinct nodes, which makes it possible for data to travel, utilizing multi-hop network paths, earlier the line of sight without counting on wired infrastructure. Security in such networks, however, is a fine difficulty [19]. The open nature of the wireless medium makes it effortless for outsiders to hearken to network visitors or intrude with it.

A wormhole attack is an above all severe attacks on MANET routing where two attackers, linked via a high-speed off-channel link, are strategically positioned at distinctive network ends, as shown in figure 1. These attackers then file the wireless data they overhear, ahead it to one another, and replay the packets on the different end of the network. Replaying legitimate network messages at incorrect places, wormhole attackers can make far aside nodes believe they are instant neighbors, and drive all correspondences between influenced nodes to through them.

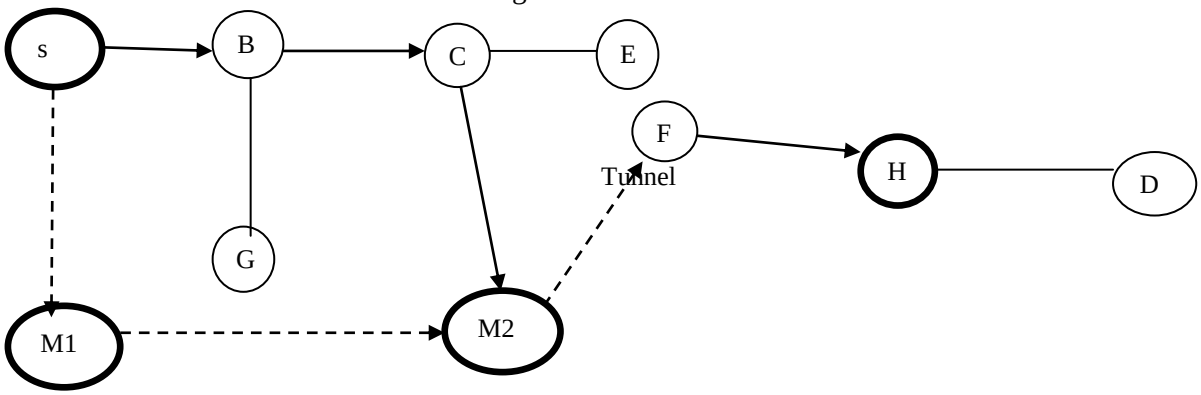

Figure 1. MANET with a Wormhole Attack

ISSN: 2233-7857 IJFGCN

More often than not, ad hoc routing protocols fall into two classes: proactive routing protocol that depends on the periodic transmission of routing packets overhauls, and on-demand routing protocols that seek for routes only when critical. A wormhole attack is equally worse a chance for each proactive and on-demand routing protocol.

2. Mobile Ad-hoc Network

2.1. Introduction

As MANET is a self configuring network with dynamic topology wherein nodes have the property to without problems deploy them within the network and change their position hence. In a MANET, each one of the most node acts as a number as well as router at the same time. Because of the shortage of centralized administration in MANETs, numerous routing attacks are suspected to be introduced in the network at any time. Security is a difficult case to handle in case of wireless networks as the mobile nodes can easily change their position and their topology is random. Different types of attacks are present in the network. The attacks can be categorized as active and passive attacks. Inactive attacks, the attackers now not handiest hearken to the data that is being transmitted but in addition they tamper the tamper the data. But in case of passive attacks, the attackers only listen the data being transmitted and use that information in a variety of ways. An extreme sort of attack in MANET is wormhole attack whose detection and prevention action is the subject of discussuion in this work. A description of the work done so farregarding wormhole attack detection and prevention has been mentioned in this paper and their solutions are also mentioned. [7]

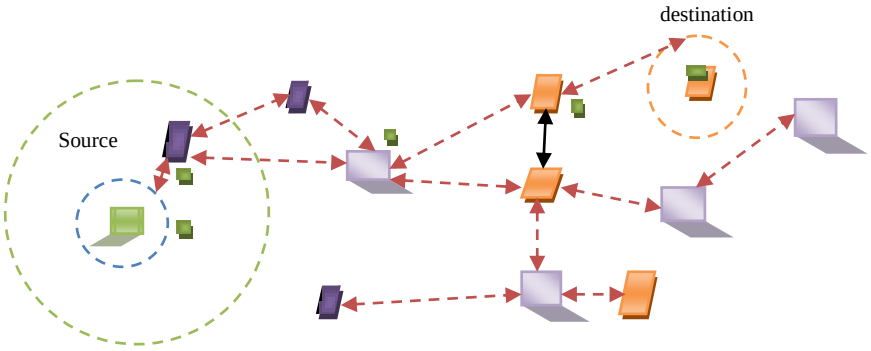

Figure 2. Example of Transmission Range source to Destination

2.2. MANET Characteristics

Distributed operation: The control of the network is distributed among the nodes; there is not any primary history for the manage of operations. The nodes must cooperate with each different and keep on communicating among themselves and each node acts as a relay as wanted, to put in force precise administrations much the same as routing and security

Multi hop routing: When a node need to send data to different nodes which is out of its correspondence range, then the packet will must be sent by means of intermediate nodes.

Autonomous terminal: In a MANET, all mobile node would function as each a router and a host in a view that is an unbiased node.

Dynamic topology: The network topology may trade randomly and at the unpredictable time; nodes are allowed to move dynamically with one of a kind rates.

Lightweight terminals: The nodes at MANET are mobile with considerably less CPU limit, low power stockpiling and little reminiscence size.

Shared Physical Medium: The wireless communication medium is offered to any entity with the correct gear and sufficient resources. [1].

2.3. Advantages of MANET*:*

The ad-Hoc network benefits [1] include following:
1. They furnish access to understanding and services regardless of geographic function.
2. Self-configuring network,, nodes are also act as routers. Independence from vital network administration.
3. Less steeply-priced as in comparison with wired network.
4. Scalable
5. Extended Flexibility.
6. Amazing
7. The network can also be without problems hooked up at any position and time.

2.4. Attacks in MANET

The wireless Channel is out there for each legitimate network users and malicious attackers.

There is no very much characterized limit where traffic is checking. There are two sorts of security attacks in MANETs.

Passive Attacks: A passive attack does not upset network ordinary operation; the attacker snoops information traded network inside without changing it. Right here the requirement of confidentiality will get violated. Detection of passive attack might be extremely complex for the operation of the network itself doesn't get influenced. One of the options of the drawback is to use strong encryption mechanism to encrypt the data being transmitted, thereby making it inconceivable for the attacker to get useful information from the data overhead.

Active Attacks: An active attack makes an endeavor to adjust or harm the data being traded in the network there with the guide of disturbing the customary working of the network. Active attacks can be inward or outer. *External attacks* are connected with method for nodes that don't have a place with the network. *Internal attacks* are from traded off nodes which are a part of the network. Considering the attacker is as of now a part of the network, internal attacks are extra extremely and tough to realize than external attacks. Active attacks, whether using through an outside advisory or an internal compromised node conclude actions corresponding to impersonation, alteration, fabrication and replication.

3. Wormhole Attack

3.1. Introduction

In wormhole attack, a passage is made between two nodes that can be used to covertly transmit packets. In a wormhole attack, an attacker gets packets at one point inside the network, burrows them to one more consider the system and after that replays them into the network from that component. For tunneled removes longer than the ordinary wireless transmission scope of a solitary jump, it's straightforward for the attacker to make the tunneled packet arrive faster than various packets transmitted over common multi-hop route, for example by means of the use of a single long variety directional wireless link or by way of a direct wired link to a colluding attacker. It is usually feasible for the attacker to forward every bit over the wormhole instantly, without waiting for an entire packet to be bought earlier than opening to tunnel the packet bits, as a way to shrink delay introduced through wormhole. If the attacker performs this tunneling truthfully and reliably, no harm is finished; the attacker clearly provides a useful service in connecting the network more efficiently. Wormhole attack is specifically damaging against numerous advert hoc network routing protocols in which nodes that hear a packet

transmission directly from some node keep in mind themselves to be in the range of (and thus a neighbor of) that node. For illustration, when used towards an on-demand routing protocol corresponding to DSR or AODV, a powerful software of the wormhole attack will also be established by means of tunneling each and every ROUTE REQUEST packet immediately to the destination target node of the REQUEST. When destination node's neighbors hear this REQUEST packet, they'll comply with typical routing protocol processing to rebroadcast that copy of the REQUEST after which discard without processing all different obtained ROUTE REQUEST packets originating from this identical Route Discovery [8]

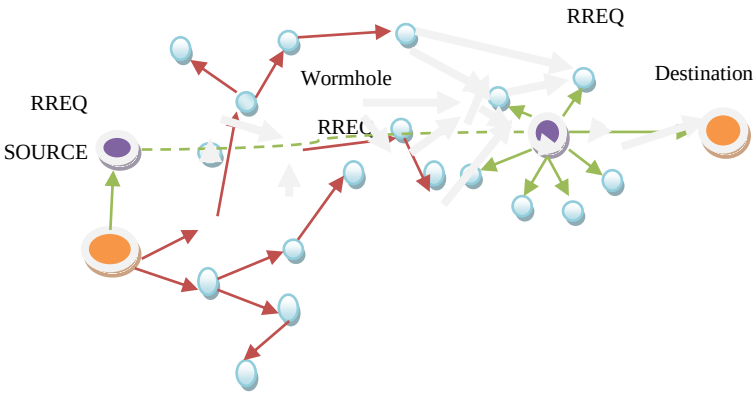

Figure 3. Wormhole Attack

3.2. Classification of Wormhole Attack

It's difficult to become aware of such dangerous attacks and no person can predict what the wormhole nodes can do and the place and when. The wormhole attack is invisible on the greater layer and thus, to finish features of the wormhole should not visible in the route wherein detection becomes rather more complex. Wormhole may also be categorized into further five categories as proposed

- Wormhole is utilizing Encapsulation.
- Wormhole making use of out of band channel.
- Open wormhole attack.
- Closed wormhole attack.
- Half open wormhole attack.
- Wormhole with high power transmission.

3.3. Wormhole Detection Techniques

A. Distance and Location Based: Packet Leash Technique

Many methods have been proposed applying a packet leash method for the wormhole attack detection. The packet leash (Yih-Chun Hu et.Al, 2003) is the system that defends towards the wormhole attack. The leashes will also be grouped both into geographical or temporal. In geographical leashes, all nodes must have knowledge of its possess vicinity in the network and secure synchronized clock. At any time when a sender sends the data packet, it entails its possess contemporary area and transmission time in the header. Consequently, the recipient is in a position of anticipating the neighbor connection by utilizing computing the separation amongst itself and source. In worldly chains, all nodes ascertain the close time of each packet by method for using light's pace and annex this termination time in the packet's header. Destination thinks about its own landing time and close time in the packet to find the wormhole attack. Geographical leashes are additional

compelling than transient rope as they don't require a firmly synchronized clock. It has the limits of GPS technology.

B. Special Hardware Based Approaches

The protected observing of Node Encounters in Multi-hop Wireless Networks (SECTOR) is a wormhole detection system that doesn't depend upon time synchronization (Srdjan Capkun et.Al, 2003). In this SECTOR method utilizes Mutual Authentication with Distance-bounding (MAD) protocol for the separation estimation between 2 nodes or users. MAD works inside the supposition that each node is added with the handset as further Hardware.

C. Localized Encryption and Authentication Protocol (LEAP)

Localized Encryption and Authentication Protocol (LEAP) is a methodology which is recommended by Zhu. This model is founded on clustering and it requires defining 4 sort key for every sensor node akin to,

A. Individual key that is shared with the base Station.
B. Pair insightful key that is imparted to a further sensor node.
C. Cluster key that is imparted to different neighboring nodes.
D. Group key that is shared with the aid of all the nodes within the network.

This method is implemented for static or motionless sensor networks.

D. Topological Technique

All around, a wireless multi hop network is conveyed to the surface of a geometrical situation, relating to a plane or a hard landscape [10]. In this procedure we enhance standards in steady area, assuming continuous deployment of nodes over the geometric surface with one-to-one mapping of the features on the outside to realize wormhole nodes. A new topology area is formed after the wormhole is glued to the original surface. We subsequently analysehow the exceptional topology areas are generated after gluing specific forms of wormholes.

- Class I wormhole, all of its two different endpoints locate within the surface (Fig. 3(a)).
- Class II wormhole has one endpoint throughout the surface and the opposite on the boundary of the skin (Fig. 3(a)).
- Class III wormhole has its endpoints on two distinct boundaries (Fig. 3(b)).
- Class IV wormhole has both of its endpoints on the same boundary (Fig. 3(c)).

E. Multipath Hop-count Analysis Technique

This model is produced through Jen which is alluded to as Multipath Hop tally analysis to limit the wormhole attack for MANETs. MHA is a process established on hop-depend analysis with the intention to avert this attack in MANETs from the standpoint of users with none detailed environment assumptions [10]. Within the MHA process first, the hop-rely values of all routes are calculated and in your next step, a dependable set of routes is chosen for data transmission. Ultimately, the packet is transmitted to the destination via the secure routes due to reducing the rate of packet that is despatched by means of the wormhole. Some of the points of this approach are that it does no longer require any designated hardware to well- done. It utilizes control packets as in RFC3561 and tries to change it. For that reason, it used the RREQ packet is used for route discovery and the RREP packet is used for route.

F. Watchdog Technique

To identify misbehaving nodes and avoids routing via theses nodes, watchdog and pathrater. On this framework, watchdog recognizes misbehavior of nodes through duplicating packets and kept up a support for as of late despatched packets. The overheard packet is in comparison with the despatched packet, if there's an in shape then discards that packet. On the off chance that the packet is timeout, increase the disappointment count for the node. What's more, if the count surpasses the edges, then the node will get into misbehave. The execution of watch dog method is demonstrated in Fig. 4

3.4. Terms to Detect Wormhole Attack

There are different forms of techniques to realize a wormhole attack on the network. Mahajn et al. [11] remember a number of terms for measuring the capability of nodes worried in wormhole attack. These are defined beneath:-

1) Strength: - it is amount of site visitors attracted through the false hyperlink advertised by the colluding nodes.

2) Length: - higher the change between the actual path and the advertise path, extra anomalies may also be determined within the network.

3) Attraction: - This time period refers back to the slash within the route size supplied by way of the wormhole. If the appeal is small then the small growth in normal direction could scale down its force.

4) Robustness:- The power of a wormhole alludes to the capacity of the wormhole to hold on without huge check inside the power even within the sight of adolescents.

4) Robustness:- The heartiness of a wormhole alludes to the capacity of the wormhole to continue without enormous control inside the power even within the sight of adolescent topology alterations within the network. Apart from these, the packet supply ratio which is the quantity of a packet of delivered divided via the whole quantity of packets dispatched varieties a basic metric to quantify the affect.

4. Techniques using Prevention and Detection of Wormhole Attack in MANET

The quite a lot of techniques used for the prevention and detection of wormhole attack in MANET is described below:

A. Packet Leashes

On this paper [2], the process is used to become aware of wormhole attack. Two varieties of Leashes: Temporal Leashes and Geographical Leashes. Temporal Leashes is centered on sending and receiving packet time from 1 node to one other node. Geographical Leashes is headquartered in nodes vicinity.

1. *Temporal Leashes:* All modes must need strongly synchronized clock. It is based on off- the -shelf hardware.

2. *Geographical Leashes:* There is no prerequisite of clock synchronization. It requires GPS hardware. In this method when one node sends a packet to another node then it add its own location ps and time on which it sends a packet ts. The receiver compares the value of sending packet with its own location pr and time at which it receives packet tr.

Directional Antennas

It is a hardware based method [2] in which all nodes are equipped with directional antennas that communicate with all other, nodes use particular sectors of antennas and observe the direction of the received signal. If the directions of both the pairs match than relation are set. This approach fails if an attacker intentionally places the wormhole between the communicating nodes.

Digital Signature

This paper is provided an approach which is priceless to hinder a wormhole attack in ad hoc network is affirm a digital signature of a sending node by receiving node. All nodes contain digital signature of every other legitimate node of the current network. Create a trusted path between sender and receiver with the help of verifying of digital signature.

On the off chance that malicious node present it is recognized on the grounds that that node does not have a legal digital signature.

Neighbour Node Analysis

In this paper neighbour node approach analyse the entire neighbour node for the purpose of authentication, so that secure transmission can be occur over the wireless network. This method is used request and response mechanism. Node will send a request to its all neighbour nodes. The node will maintain a table which stores a reply time. If reply time is notaccurate there is a harmful node in the current network. The reaction time of RREP message is contrast with the reaction time of real message sent. If the response time of specific message is greater than the response time of RREP + threshold worth than we will say that wormhole link is reward within the route. Assessment of this method is repeated until destination reached.

DelPHI technique

Delay Per Hop Indication is established on the calculation of (delay per hop) worth of disjoint paths. It is based on the fact that under normal condition, the delay a packet experiences in propagates one hop should be comparable along each hop path. At the same time in wormhole attack, the prolong for propagating throughout fake neighbours are excessive as there are a lot of hops between them. It doesn't want any further hardware or tight time synchronization and has high energy efficiency. It works for both In-Band and Out of –Band mode.

WHOP technique

This paper proposes a routing protocol WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on AODV. In WHOP, a hound packet will probably be sent after the route has been uncovered utilizing AODV routing protocol, the hound packet shall be processed via each node besides nodes who were involved in route from source to destination during path set up. WHOP contains another three column address of node processing bit (PB) and count to reach next hop (CRNH). CRNH represents the hop difference between neighbors of one hop separated node; its price can be increment with the aid of every node for the first node entry whose processing bit is zero in the packet.

Table 1. Summary of Detection Methods of Wormhole Attack. [18]

Method	**Mobility**	**QoS Parameter**	**Synchronization**	**False detection**
HMTIs	Taken care of weakly. Topologically robust, short range worm-gap can be identified.	Jitter and delay.	Not required science psc profile is	Used PSD to detect false positive alarm.

			done	
Farid et al.	Not considered.	Packet handling time, line delays inside nodes.	Some time delay added to detect suspicious links.	Not handled.
DelPHI	Not considered.	Delay.	Not required.	Not handled.
SAM	Cluster and uniform topology considered.	Not considered.	Not considered.	Not handled.
SaW	Not considered	Not considered.	Not considered.	Failed to detect.
DaW	Not considered.	Delay parameter.	Not considered.	Failed to detect.
WAP	Maximum transmission distance is calculated.	Delay per hop.	Only the source node is synchronized.	Not handled.
WORM EROS	Topological change is not considered.	Not considered.	Time synchronizatio n no longer required. RTT between source node and destination node is considered	Both false c positive and false negative are viewed.

5. Literature Survey

In [12] security has emerged as a predominant problem with the intention to provide covered communication between mobile nodes in a opposed atmosphere of MANET which poses a number of nontrivial challenges to protection design and these challenges naturally make a case of constructing multifence safety solutions that accomplish both broad protection and attractive network execution. This paper shows a survey on the different network layer attacks, i.e. Wormhole attack, blackhole attack and greyhole attack and present methods to mitigate them.

In [14] quite a lot of attacks feasible in MANEt wormhole attack is one which is handled as an awfully severe attack. In this attack a malicious node records packets in one location in the network and tunnels them to a further malicious node which is reward in the various finish of the network. In this paper, have proposed an algorithm which detects

and avoids the wormhole attack in the routing phase itself. Our mechanism is centered on the total round trip time (RTT) of the founded route and the usual circular commute instances of the sender one hop neighbors, which is considered as highest one hop round trip time. Our solution works for each MANETs and wireless ad hoc networks.

In [3] attacks may lead to either misdirection of data traffic or denial of services. The mitigation tactics to combat the attacks in MANETs need to work beneath extreme constraints, and hence it is vital to learn the vulnerabilities of the routing protocols and ways of launching the attack in detail. This paper makes an attempt to do the equal and has reviewed some current literature on mitigation of the routing attacks.

In [13] lack of centralized authority safety in MANETs is very difficult. Usually, routing protocols were designed for better efficiency most effective and security issues were not regarded. So either new routing protocols will have to be designed which have protection parameter also or security parameters have got to be integrated within the current routing protocol. There are a number of attacks on routing protocol, one of them is wormhole attack.

We will be able to overview the performance of AODV and DSR routing protocol beneath wormhole attack and compare the performance of those protocols without wormhole attack. Performance parameters are average end to end prolong, Throughput, and Packet delivery ratio(PDR). We will be able to use Qualnet Simulator 5.0.

In [4] MANETs are infrastructureless. As such, they are subject to various types of security attacks if malicious nodes are present in the network. One of such attacks is the wormhole attack. In an earlier work, a scheme (called Cell-based Open Tunnel Avoidance (COTA)) was proposed to address this problem, which consisted in a mechanism for detecting and classifying the wormhole attacks in the network. In this paper, the COTA mechanism is implemented on the location aided routing protocol (LAR1), leading to the so-called COTALAR1 scheme. Simulation outcome is offered, displaying that the COTA-LAR1 scheme is a multiplied secured routing scheme towards wormhole attacks in MANETs, in phrases of packet delivery ratio, throughput, and end to-end delay, picked as proficiency metrics.

In [15] process works in three stages, which can be making utilization of route redundancy, route aggregation and ascertaining round-trip time (RTT) of all recorded routes. Routes redundancy is began where supply sends RREQ using every possible approach to destination. All courses that join source and destination are recorded close by the quantity of hops from each course. Some courses accumulated in the equivalent hand-off component before the destination is totaled, so all nodes that join the network may likewise be recorded and the propensities for malicious nodes in may likewise be distinguished. The RTT and number of hops of all listed routes are when put next in an effort to realize suspicious route Nodes with suspicious conduct within the network are remoted and will not be viewed for transmission. Recreation results recommend the capacity to confine the expanding of packets dropped, headquartered on wormhole seclusion in our proposed plan contrast with normal AODV protocol and procedure of prior time-established calculation..

In [20] work, some modifications have been done in AODV routing protocol to detect and remove wormhole attack in real-world MANET. Wormhole attack detection and prevention algorithm, WADP, has been executed in adjusted AODV Also node authentication has been utilized to recognize malicious nodes and evacuate false positive issue that may emerge in WADP algorithm. Node authentication expels false positive as well as aides in the mapping careful area of wormhole and is a sort of double verification for wormhole attack detection. Simulation results prove the theory.

In [16] find which protocol is more vulnerable to the wormhole attack. The OPNET simulation outcome shows the throughput, finish-to-finish delay, network load and traffic received with Wormhole and without Wormhole on AODV and OLSR in MANET. The outcome exhibit that AODV is more liable to wormhole attack in comparison with OLSR.

Therefore, the application of MANET that uses a proactive routing protocol is more trusted compared to the reactive one.

In [9] wormhole attack launched through exploiting AODV protocol in the MANET, is detected and removed in two phases. The preliminary phase in the identifying wormhole attack procedure is done, based on timing analysis and hop count. After suspecting attack, a Clustering based process is used to verify the attack presence, and in addition to establishing the attacker nodes. The complete network is divided into various clusters and every cluster will have a Cluster Head, which controls all the nodes in the cluster and perform the role of a controlling authority in MANET.

In [5] Procedures dealing with wormhole attack detection and technique for wormhole detection and prevention are proposed. A proposed process is centered on the Hash based Compression function (HCF) which is surely using any relaxed hash perform to compute a worth of hash subject for RREQ packet. Proposed technique appears very promising compared to other viable options in literature survey. All the simulations will be performed on the NS2 simulator using AODV reactive routing protocol.

In [21] environment, the presence of malevolent nodes may result in wormhole attacks. In this paper, a secured AODV-based routing scheme (referred to as Timed and Secured Monitoring Implementation – (TSMI)) is proposed for mitigating such attacks. Simulation outcome is offered to illustrate the effectiveness of our method, making use of the packet delivery ratio, the number of damaged links detected, and the quantity of packets obtained by destination, as efficiency warning signs.

In [6] lack of critical factor of control, MANETs are extra prone to routing attacks as compared to other networks. Wormhole attack is one of the most extreme routing attacks, Which is convenient to enforce but tough to detect. Almost always, it really works in two steps; in step one, the wormhole nodes attract more and more site visitors closer to them by way of the wormhole channel, and inside the second step, they start hurting the network by utilizing adjusting or dropping the network traffic. A few authors have proposed unique options to counter wormhole attacks in MANETs. In this paper, we completely analyze these current procedures on the groundwork of their boundaries as well as elements that are valuable in detecting wormhole attacks in MANETs.

In [17] contains a proposition for new strategy for wormhole evasion. Tha proposed method has been executed with the NS2 test system over the DSR protocol. This system for wormhole shirking addresses the malicious nodes and evades the routes having wormhole nodes without influencing the general execution of the network. The execution metrics utilized for evaluating network execution are jitter, throughput and end to end delay. The execution of proposed systems is good.

6. Proposed Work

In this work, we have a tendency to planned a trust and reputation management theme for verifying the trustworthy location in Manet atmosphere. Evaluating the trait of RREQ in Manet still remains as associate degree open downside up to now. Recently, reputation and trust management has been planned as technique to wear down many of those deficiencies. This planned technique is employed for characteristic the trustworthy location. To judge the trustworthy location we have a tendency to introduce the trustworthy and name based mostly mechanism exploitation Bachelor of Science (base station). During this planned framework, a majority mining scheme/technique and Bachelor of Science square measure accustomed calculate for characteristic the unsuspecting message. They supply foundations for estimating the trait of a message. During this theme, the simulation results show that our planned work will effectively filter bastard messages and verify the trustworthy location and this schemed performs satisfactorily within the realistic atmosphere.

1**)** We have a tendency to planned a trust and name management theme for verifying the trustworthy location in Manet atmosphere.
2) To measure the trustworthy location we have a tendency to introduce the trustworthy and name based mostly mechanism exploitation Bachelor of Science (base station).
3) In this planned framework, a majority mining scheme/technique and Bachelor of Science square measure accustomed calculate or characteristic the unsuspecting message. They supply foundations for estimating the trait of a message.
4) On this theme, the simulation results show that our planned work will effectively filter bastard messages and verify the trustworthy location and this schemed performs satisfactorily within the realistic atmosphere.

7. Result Simulation

In simulation work use of ns-2.35 on AODV routing protocol below table shows the simulation parameter.

Simulation tool	Ns-2.35
Protocol	AODV
Queue size	20
Mac	802_11
X	1000
Y	1000
Stop time	100ms
Number of nodes	14
Antina	Omnidirectional

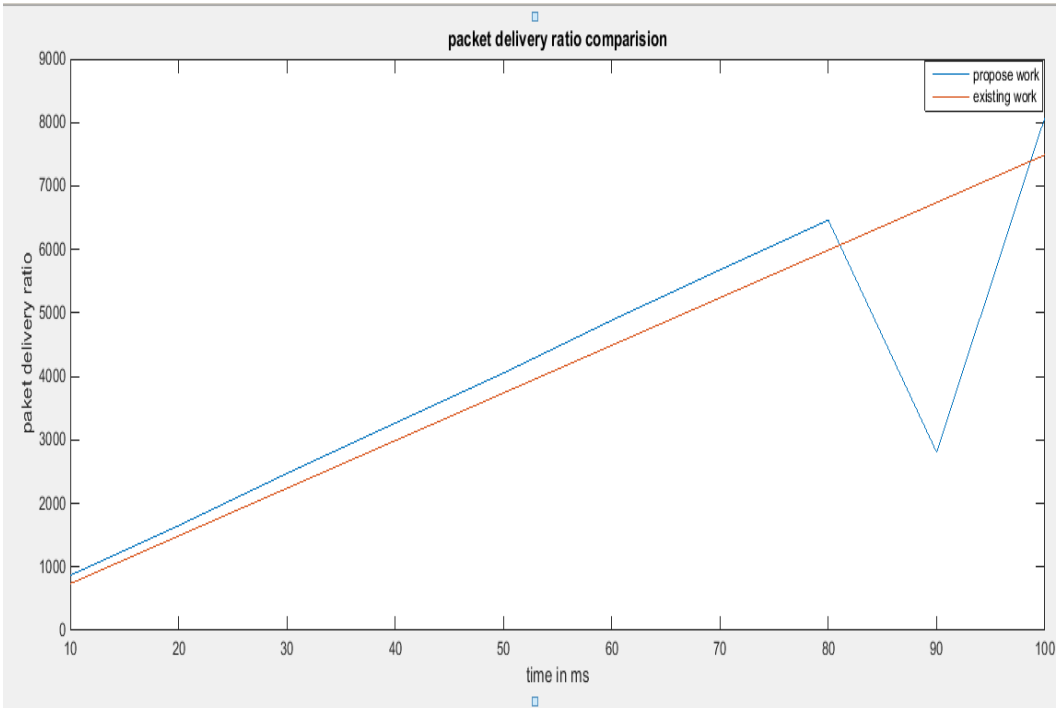

Figure 4. Packet Delivery Ratio

In fig 4 shows comparison between existing and proposed work over packet delivery ratio. Here blue show proposed work and red shows existing work.

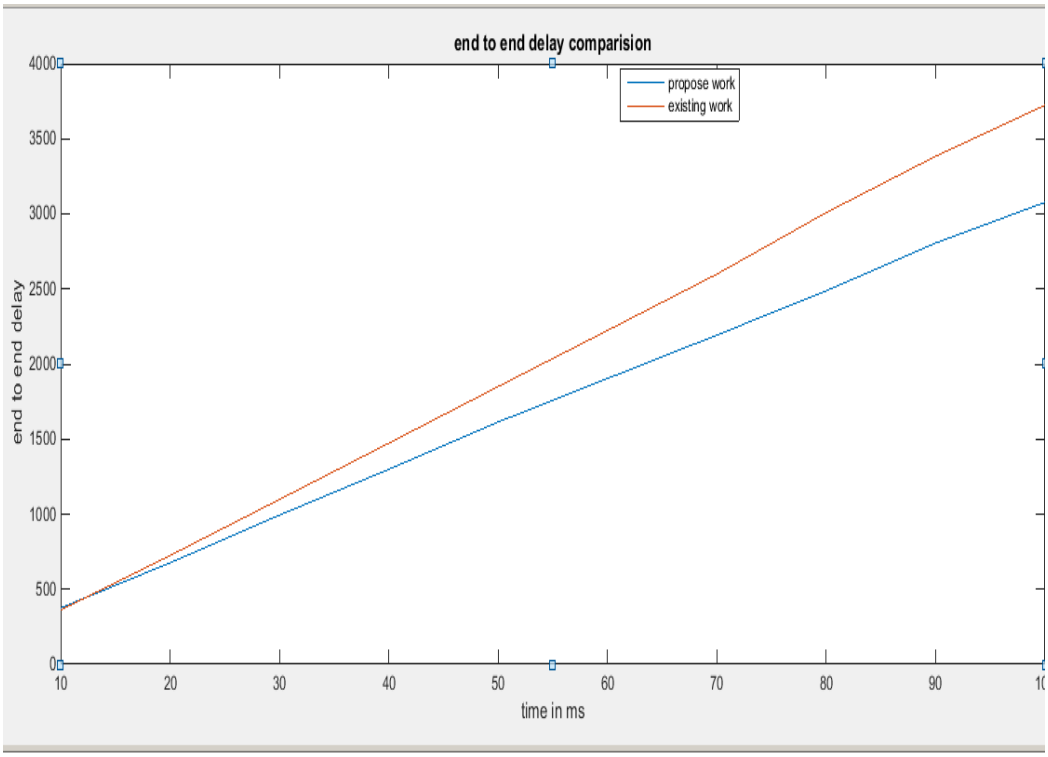

Figure 5. End to End Delay

In Figure 5 shows a comparison between the existing and proposed work over End to End delay. Here blue show proposed work and red shows existing work.

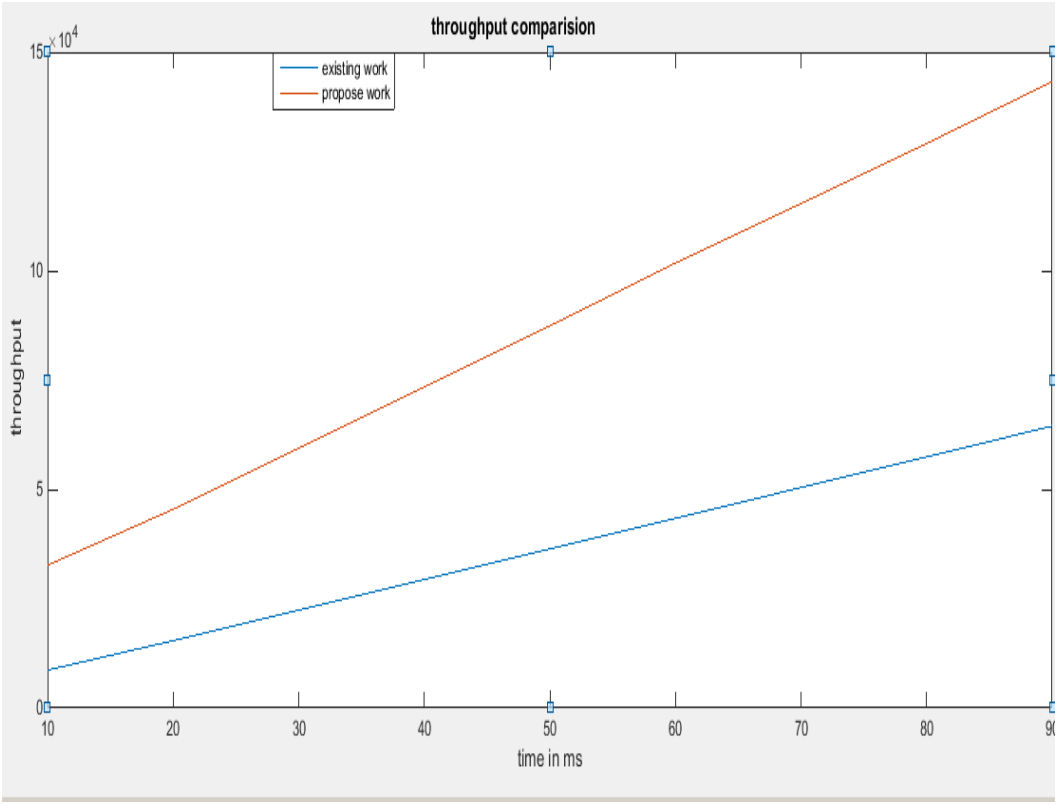

Figure 6. Throughput

In Figure 6 shows comparison between existing and proposed work over Throughput. Here blue show proposed work and red shows existing work.

Conclusion

In propose work we implement on NS-2.35 on the basis of result we conclude that our propose work perform better compare to existing technique, in future work we apply optimization techniques to improves our result.

References

[1] D. Patel, P. Trivedi and M. B.Potdar, "A Brief Analysis on Detection and Avoidance Techniques of Wormhole Attack in MANET", International Journal of Computer Applications (0975 – 8887), vol. 117, no. 16, **(2015)**.
[2] D. Sorathiya and H. Rathod, "A Review on Detection and Prevention Techniques of Wormhole Attack in MANETs", International Journal of Science and Research (IJSR), vol. 4 iss. 1, **(2015)**.
[3] R. K. Kapur and S. K. Khatri, "Analysis of Attacks on Routing Protocols in MANETs", 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) MS Engineering College, Ghaziabad, India IEEE, pp. 791-798.
[4] V. Teotia, S. K. Dhurandher, I. Woungang and Mohammad S. Obaidat, "Wormhole Prevention using COTA Mechanism in Position Based Environment over MANETs", IEEE ICC 2015 - Communications Software, Services and Multimedia Applications Symposium, pp. 7036-7040.
[5] A. Patel, N. Patel and R. Patel, "Defending Against Wormhole Attack in MANET", 2015 Fifth International Conference on Communication Systems and Network Technologies, pp. 674-678.
[6] M. Imran, F. A. Khan, T. Jamal and M. H. Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs", International Workshop on Cyber Security and Digital Investigation (CSDI 2015), pp. 384 – 390.
[7] Aashima and V. K. Arora, "Detection and Prevention of Wormhole Attack in MANET Using DSR Protocol", IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, iss. 6, ver. VIII, **(2014)**, pp. 44-47.
[8] A. Jain and A. J. Tiwari, "A Combined Approach for Worm-Hole and Black-Hole Attack Detection in MANET", Amber Jain Int. Journal of Engineering Research and Applications, vol. 4, iss. 9 (Version 1), **(2014)**, pp.18-22.
[9] J. Anju and C. N. Sminesh, "2014 3rd International Conference on Eco-friendly Computing and Communication Systems", 2014 IEEE, pp. 149-154.
[10] Y. Gohil, S. Sakhreliya and S. Menaria, "A Review On: Detection and Prevention of Wormhole Attacks in MANET", International Journal of Scientific and Research Publications, vol. 3, iss. 2, **(2013)**, pp. 1-6.
[11] J. Thalor and M. Monika, "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, iss. 2, **(2013)**, pp. 137-142.
[12] G. Garg, S. Kaushal and A. Sharma, "Comprehensive Study On Manets Network Layer Attacks", IEEE, ICCCNT, **(2013)**.
[13] R. Ahuja, A. B. Ahuja and P. Ahuja, "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack", Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), pp. 699-702.
[14] V. K. Raju and K. V. Kumar, "A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks", 2012 International Conference on Computing Sciences, IEEE, pp. 271-275.
[15] S. Y. Shin and E. H. Halim, "Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation", IEEE, **(2012)**.
[16] M. Sadeghi and S. Yahya, "Analysis of Wormhole Attack on MANETs Usingn Different MANET Routing Protocols", IEEE, **(2012)**, pp. 301-305.
[17] Y. Singh, A. Khatkar, D. P. Rani and D. D. Barak, "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks", IEEE, **(2012)**, pp. 283-287.
[18] R. Maulik and N. Chaki, "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications, vol. 3, **(2011)**, pp. 271-279.
[19] D. B. Roy, R. Chaki and N. Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), vol. 1, no. 1, **(2009)**.
[20] J. Biswas, A. Gupta and D. Singh, "WADP: A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol".
[21] I. Woungang, S. K. Dhurandher, M. S. Obaidat and I. Traore, "A Timed and Secured Monitoring Implementation AgainstWormhole Attacks in AODV-Based Mobile Ad Hoc Networks", IEEE.

