A Trust based Approach for Detection and Prevention of Wormhole Attack in MANET

Kamini Singh
IT Department
IET-DAVV,Indore

Gyan Singh
Computer Science Department
MITM, Indore

Arpit Agrawal
Computer Science Department
IET-DAVV, Indore

ABSTRACT
As in wireless network there is necessity of nodes cooperation to transfer packets from one node to another this property makes it vulnerable to wide range of attacks at different layer. Wormhole attack is one of the most destructive severe attack in which malicious node captures the traffic at particular location and tunnels it to another part of tunnel that is far away. In network security is generally equated by strong and feasible authentication and adopting methods of encryption and decryption.However this attack is hardly defeated as they do not use any additional effort to deploy nor create any extra packets. They simply capture packets then either drop them or replay in existing network, which make them to pass from any type of cryptographic checks and authentication Work done in this field have generally focused on use of additional hardware like directional antenna. In this paper, we present a cluster based counter-measure for the wormhole attack that alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET. Simulation results shown on NS2 display the effectiveness of the proposed method for detecting and preventing wormhole attack.

Keywords
MANET, Wormhole, Cluster, Monitor Node, Routing.

1. INTRODUCTION
An ad-hoc network is infrastructure-less self-organized network system, in which each nodes actas both host and router at a time i.e. each node forward data packets to other nodes and decides to which node it should forward data next based on the network connectivity.Because of infrastructure-less environment now days ad-hoc network is widely used ,many applications work in untrusted environments and some require secure communication and routing such as emergency response operations like a flood, tornado, hurricane or earthquake and military or police networks,. But, the open nature of the wireless communication channels, the fast deployment, the lack of infrastructure, and the environment where they may be deployed and make them vulnerable to a wide range of security attacks.figure 1 shows a simple ad-hoc network in which nodes A and C discover the route through node B for communication. The circles boundary indicates the range of each node. Nodes A and C are not directly in each other transmission range, since A's boundary does not include node C [2].

There are many attacks in network on different layers such as DOS attack, sniffing, etc. Among different attacks one of the severe attack is *wormhole.* During this attack, a malicious node captures packets from one location in the network and "tunnels" them to another malicious node at a distant point which replays them locally.Tunnel can be established in many ways like in-band and out-of-band channel [1]. This leads tunneled packet to reach destination sooner in much less time and with less number of hop count compare to normal routing.

1.1 Routing Protocol
The main function at IP layer of MANET is to perform end-to-end delivery of data i.e. from source to destination. A routing protocol for MANET should have following features [3]:

1. It must be distributed as centralized routing, involves high control overhead and it is not scalable.

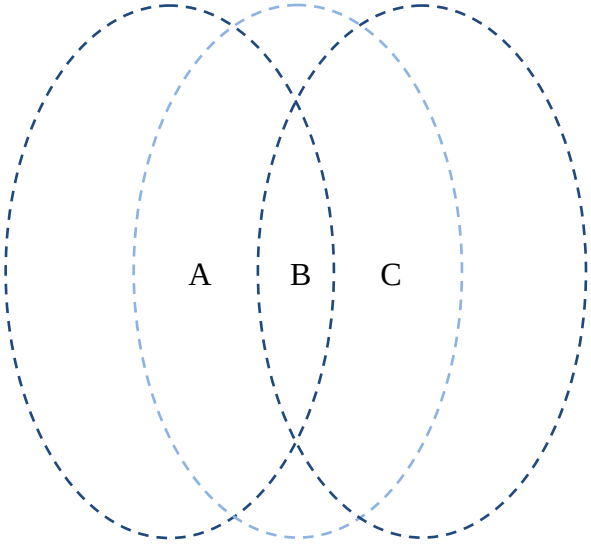

Fig.1 Example of a simple ad-hoc network [2]

2. It must be adaptive to frequent topology changes caused by the mobility of nodes.
3. Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes; it means minimum connection setup time is desired.
4. It must be localized, as global state maintenance involves a huge state propagation control overhead.
5. It must be loop-free and free from stale routes.
6. It must converge to optimal routes once the network topology becomes stable.
7. It must optimally use scarce resources such as bandwidth, memory, computing power and battery power.
8. Every node in the network should try to store information regarding the stable local topology only.

1.2Classification of Routing Protocols
1.2.1 Proactive or table driven routing protocol
In table driven routing protocol each node maintains the network topology information in form of routing tables periodically by exchanging routing information to maintain consistent and up-to-date view of the network when topology is changes. When the node requires a path to destination it runs appropriate path finding algorithm. Routing table uses

sequence number to find latest route. Some existing proactive protocols are Destination Sequence Distance Vector (DSDV), Global State Routing (GSR), and Clustered Gateway Switch Routing (CGSR) [6].

1.2.2 Reactive or on-demand routing protocol

Protocols under this category do not maintain topology information and said as a lazy approach to routing. Route is established when it is required, they do not maintain any routing information nor exchange information periodically. The route remains valid until the route is no longer needed. Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector Routing (AODV) are routing protocol of this category.

1.2.3 Hybrid routing protocol

Hybrid routing protocol combines best features of above two protocol categories. Within a certain geographical domain a table driven approach is used and beyond this domain on-demand approach is applied. Examples are Zone Routing Protocol (ZRP), Wireless Ad hoc Routing Protocol (WARP).

1.3 Wormhole Attack

A wormhole attack[5] is the severe attack that occurs between two malicious nodes via in band or out of band channel connectivity. First adversary receives packets at one location and tunnel them to next adversary at another location.it is a type of denial of service attack that can affect the network. For example in the figure 2, the source node (S) sends packets to destination through the normal path (S-A-B-C-D),but these packets also eavesdrops by the first malacious node(X) and then tunneled to second malacious node (Y). now Y transmits them to the destination node (D) before they arrived to D from the normal path. So rest of packets that follow the normal path will be dropped by destination.

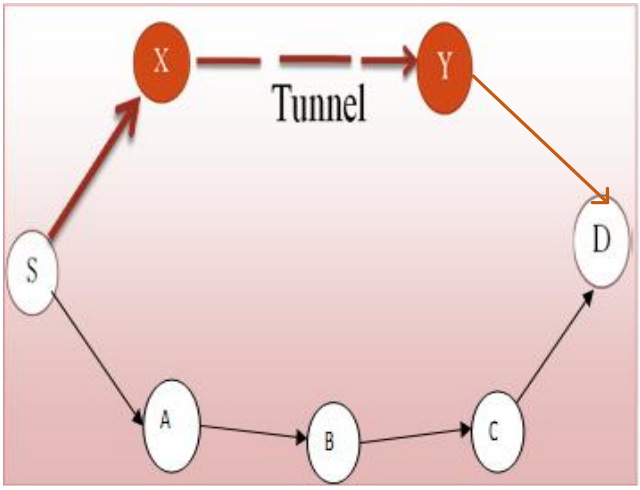

Fig.2 Wormhole Attack

2. RELATED WORKS

Security in ad-hoc networks is one of the major issue, and it is generally seen same as strong and feasible authentication and light cryptography. Many works has been done in field of security against wormhole attack in MANET.

Table.1 Comparison of Techniques [6]

Techniques	Advantages	Disadvantages
Localized algorithm	Two Conflicting sets of each node filter out incorrect distance measurements.	Works only incase of no packet loss which is unavoidable when the system is under wormhole attack
Graph Theoretical Approach	Use of encryption techniques	Guard node uses local broadcast keys which are available only in one hop neighbors.
DELPHI	1. Both delay & hop count is measured 2. Synchronization is not required	1. Rescheduling of a packet propagating one hop is very high. 2. False alarm is not detected.
HMTI	1. False positive alarm problem is solved. 2.Synchronization is not required	Jitter is to be calculated. This jitter surrounds the HMTI.
SAW & DAW	Arithmetical Trust based security model is used.	Failed to detect false alarm detection.
Cluster based	1. Guard nodes are used to in-form cluster heads about the attack. 2.Nospecial hardwires are used.	It is only applicable for layered architecture of the network.
Beacon node	1. Beacon nodes are used & their location is known. 2. Calculation cost is low. 3. It provides very low localization error.	It is only applicable for layered architecture of the network.
EDWA	Shortest path is identified	Always the routing table & the packet header are checked for Request-Reply procedure.
SAM	Probability Mass function is used for identifying Wormhole Attack	If any real neighbor connection is wrongly labeled as wormhole false positive alarm will be caused
Trust Based Model	Trust values are used for modification of the path next time	This system is robust only when time and trust based modules are combined together

3. PROPOSED METHODOLOGY

A new infrastructure is developed for the avoidance of wormhole attack which is able to detect and prevent the attacks. Objective is to detect the malicious node that performs attack.

Assumptions

a. MANET consists of clusters of nodes.
b. A node interacts with its 1-hop neighbors directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
c. Every node has a unique id in the network, which assigned to a new node collaboratively by existing nodes.
d. The entire network is geographically divided into a few disjoint or overlapping clusters.
e. Each cluster is monitored by only one cluster head (monitoring node).

3.1 Cluster Formation

In the proposed model nodes and devices are organized using a fixed infrastructure of MANET devices, where devices are categorized in the following manner.

3.1.1 Mobile nodes

These nodes are a collection of the mobile devices and follow the law of independent mobility; these nodes are those who actually use the network and their services. These nodes are frequently participates in data communication. Sending, receiving and routing data during communication sessions as the tradition of the MANET. But they only receive services from the nearest cluster heads.

3.1.2 Cluster Heads

These nodes are basically static access points which installed separately by the service provider. These nodes are participating in communication when intra-cluster communication occurs. The primary objective of these cluster heads is to monitor the communication between trusted nodes,when the new mobile node trying to communicate with internal cluster or trusted node then data sending and receiving is the main responsibility of these nodes.

3.1.3 Monitoring server

This device is used to calculate the trust value for securing the network from attack. In addition of that these nodes are also responsible for elimination of nodes that are performing malicious activities in the network.

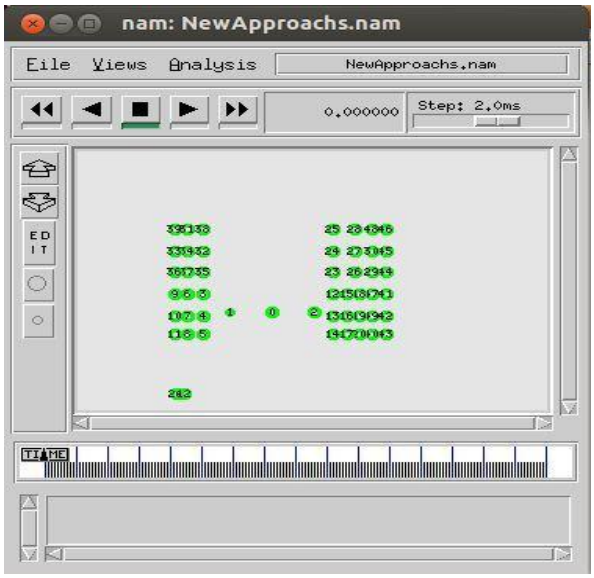

Fig.3 Show the proposed network

3.2 Wormhole Detection Procedure

1. Begin the network with two clusters and each cluster with some nodes.
2. Node with minimum node id becomes Cluster Head.
3. The node nearest to both cluster heads is chosen as Server node (Guard node).
4. Assumed that current nodes cluster is not malicious, working begins when new node wants to enter in the cluster.
5. When new node enters in the cluster first of all it is checked whether it is trusted or not, this authentication is done via following way:
6. Server node has responsibility of authentication, new node say node 21 shown in fig 4 enters, and then data is made flow through it for verification purpose.
7. If node forwards the data packets then trust value is increased otherwise decreased, at last of the trust value is compared with the defined threshold value.
8. If node is authenticated then it is included in data transmission path and if not then node id is deleted i.e. node is not included in data transmission path.

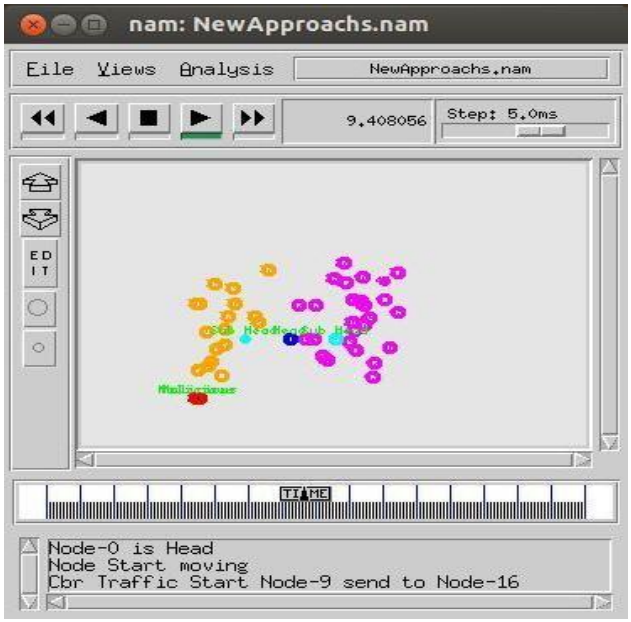

Fig.4 New node entering in Proposed Cluster Network

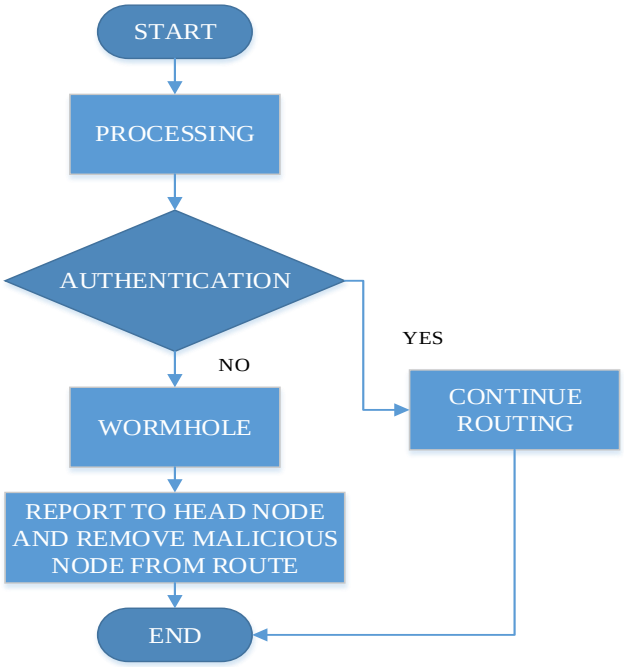

Fig.5 Detection of malicious node

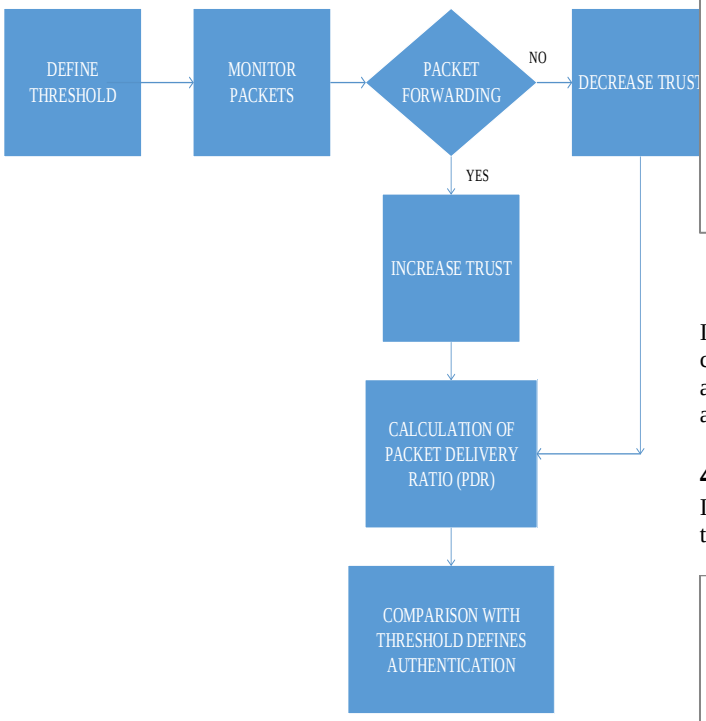

Fig.6 Showing Functionality involved in processing step

4. PERFORMANCE ANALYSIS

A Simulation study has been done in NS2.

Table.2 Simulation Parameter

Examined Protocol	AODV
Simulation Time	20ms
Simulation Area	750x500
Number of Nodes	50
Malicious Node	21,22
Number of Wormholes	1

4.1Packet Delivery Ratio

Ratio of the number of delivered to the number of sent data packets to the destination.

PDR= ∑ Number of packet receive / ∑ Number of packet send

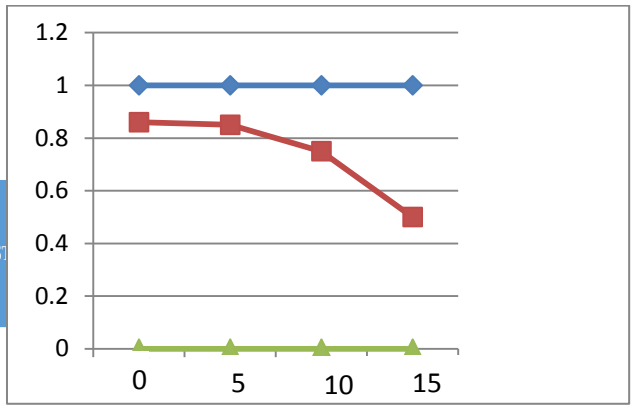

Fig. 7 Packet Delivery Ratio

In fig 7 the blue shows packet delivery ration in normal condition of AODV , green in case of attack while red tells about the ratio in case of proposed modified AODV under attack.

4.2Throughput

It defines how much data can be transferred from one location to another in a given amount of time.

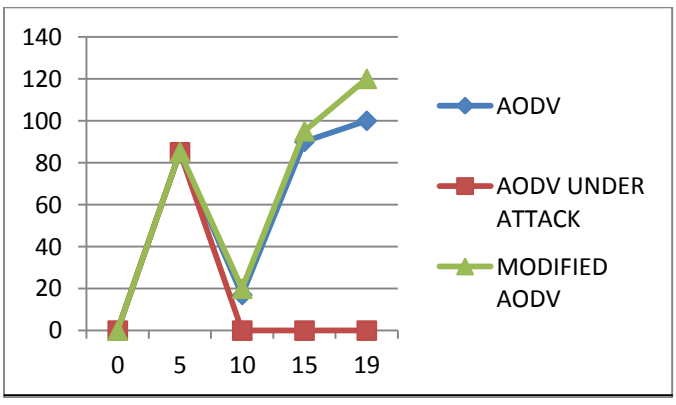

Fig. 8 Throughput

4.3 End-to-End Delay

Average time taken by a data packet to arrive at the destination. It also includes delay caused by route discovery process and queue in data packettransmission. Data packets that successfully delivered to destinations are counted only.

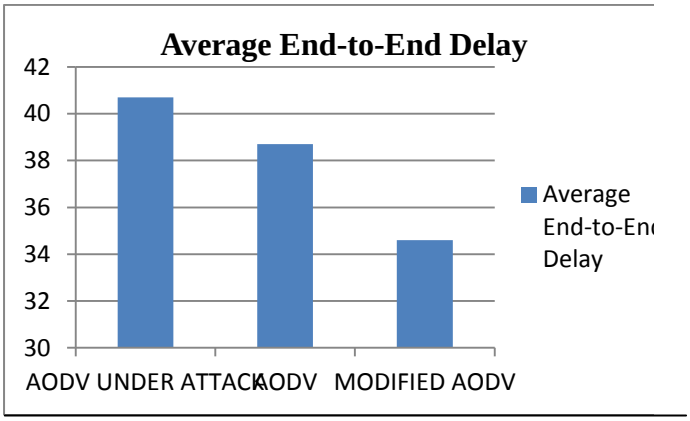

Fig. 9 Average End-to-End Delay

5. CONCLUSION

In this paper, a new cluster based wormhole detection and preventation method has been proposed. In wireless systems, there is requirement that nodes cooperate with each other for transferring data packets from one node to another which make it attractive for attacker to launch attack in network. The proposed method is able to detect malicious node on the basis of rate of packet dropping via comparing to threshold value.

The malicious nodes are excluded from the route routing for data transfer. In future this idea can be expanded by spreading the knowledge of malicious nodes in whole network.

6. REFRENCES

[1] Ajay PrakashRai, VineetSrivastava and Rinkoo Bhatia "Wormhole Attack Detection in Mobile Ad Hoc Networks"in International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 22773754 Volume 2,Issue 2, August 2012.

[2] AnjuGill,ChanderDiwaker "Adhoc Network Behavioral Study of Issues And Challenges In Mobile" IJARCSSE, Volume 2, Issue 5, May 2012.

[3] C.Siva Ram Murthy and B.S.Manoj"Ad Hoc Wireless Networks Architectures and Protocols".

[4] YudhvirSingh,AvniKhatkar, Prabha Rani, Deepika, and DheerDhwaj Barak "Wormhole Attack Avoidance Technique inMobileAdhoc Networks" in IEEE 978-0-7695-4941-5/12 $26.00 (2013).

[5] M .Sookhak ,M.R. Eslaminejad, M. Haghparastand I.in FauziISnin "Detection of Wormhole in Wireless Adhoc networks" IJCST , Volume 2, Issue 7, October 2011.

[6] Moutushi Singh, Rupayan Das "A Survey of Different Techniques for Detectionof Wormhole Attack in Wireless Sensor Network" IJSER,Volume 3, Issue 10, October 2012.

[7] L. Sudha Rani, R.RajaSekhar (Ph.D) "Detection andPreventation of wormhole in Stateless Multicasting" International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012.

[8] Kamini Singh, Gyan Singh "Review on Wormhole Security and Their Detection Scheme" IJARCSSE Volume 4, Issue 1, January 2014.

[9] MajidMeghdadi, SuatOzdemir and InanGüler ―A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks‖ ,in IETETECHNICAL REVIEW,VOL 28 , ISSUE 2 ,MAR-APR 2011.

[10] Debdutta Barman Roy, RituparnaChaki, NabenduChaki "A New cluster-Based Wormhole Intrusion Detection Algorithm for MANET"IJNSA, Volume 1 April 2009.

[11] YashpalsinghGohil, SumeghaSakhreliya, and SumitraMenaria , "A Review On:detectionand prevention of wormhole attack in MANET" , International Journal of Scientific and Research Publications, Volume 3, Issue 2, ISSN 2250-3153 , February2013.

[12] http://harrismare.net/2011/07/14/packet-delivery-ratio-packet-lost-end-to-end-delay.