New Approach through Detection and Prevention of Wormhole Attack in MANET

*** Aditi Dawane**
**** Hemant Kumar Gupta**

ABSTRACT

A mobile ad hoc network (MANET) comprises of an assortment of wireless mobile nodes that frames a brief system without having any fixed foundation or unified organization. MANET is foundation less, need of concentrated checking and dynamic changing network topology. MANET is exceptionally powerless against attack because of open mistake inclined shared wireless medium. This paper contains the detection and prevention of wormhole attack for AODV routing protocols. Our observations regarding the behavior of the above protocol, in large-scale Mobile Ad hoc Networks (MANETs) and from the analysis it is clear that the trust-based algorithm to send data to the leader proof to offer more reduced drop packets and also increase the lifetime of the network. Based on the analysis of this simulation results, Trusted Ad-hoc on-demand distance vector (TAODV) protocol offer a better solution to quality of service usage in a MANET.

Keywords: - Wormhole Attack, MANET.

* Aditi Dawane, Research Scholar, Dept OF CSE, Lakshmi Narain College of Technology and Science(RIT), Indore, MP, India, dawane.aditi@gmail.com
** Hemant Kumar Gupta, Asst. Professor & HOD, Dept OF CSE, Lakshmi Narain College of Technology and Science(RIT), Indore, MP, India, hemugupta3131@gmail.com

I. INTRODUCTION

An ad hoc network is a group of communications devices or nodes that communicate with each other without fixed topology (infrastructure) and without pre-determined organization. Hence one can define the ad hoc network as dynamic network [1]. Individual nodes have capacity to communicate directly with other nodes. An ad hoc network can be created by using wireless technologies such as Bluetooth, Wi-Fi etc. such a network is called wireless ad hoc network [2].

Mobile wireless network is the infrastructure less mobile network, commonly known as an ad-hoc network. Infrastructure less networks have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner [3]. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network. Example applications of ad-hoc networks are emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrains [4].

II. ROUTING PROTOCOL

Source-Initiated On-Demand Routing

A different approach from table-driven routing is source-initiated on demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is maintained by some form of route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired [7].

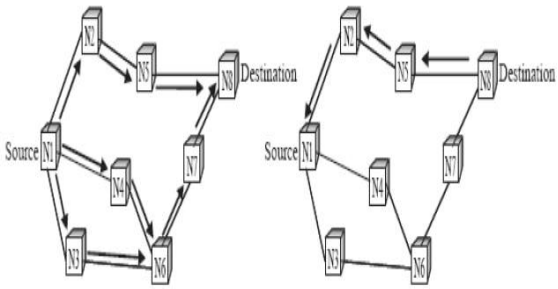
Ad-hoc On-Demand Distance Vector Routing (AODV)

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol described in builds on the DSDV algorithm previously described. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm [9]. The authors of AODV classify it as a pure on-demand route acquisition system, as nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges [9].

When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a Path Discovery process to locate the other node. It broadcasts a route request(RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. Figure 1 a illustrates the propagation of the broadcast RREQs across the network. AODV utilizes destination sequence numbers to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies a RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ [11].

During the process of forwarding the RREQ, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these

packets are discarded [3]. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination/intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ (Figure 1b). As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forwarded along the path established by the RREQ, AODV only supports the use of symmetric links.



(a) Propagation of the RREQ (b) Path of the RREP to the source

Figure 1: AODV Route Discovery

III. WORMHOLE ATTACKE IN MANET

Wormhole attack is a severe security threat to MANETs. Wormhole attack in MANETs is one of the main attacks in which a malignant node entraps the packets from a single position in the network so that they can be tunneled to another malignant node at a far-off point. In a wormhole attack, since attackers are directly connected with each other, they can, therefore, communicate at a fast speed in comparison to the other nodes in the MANET [9]. However, for the implementation of such communication, there is a need for support of special hardware. For the tunnel distances that are more than the single hop normal wireless transmission range, it is easier for the attacker to compose packets in the tunnel as compared to a regular multi-hop route. This is done due to the use of a single long-range directional wireless link or direct wired link. It is also achievable for an attacker in the wormhole attack to move forward every bit directly without waiting for receiving of the complete packet. Wireless transmission nature also makes it possible for the attacker to construct a wormhole for packets that are not addressed to it; this is possible as an attacker can overhear these packets in wireless communication and tunnel them in order to collude attacker at the other end of the wormhole [12].Wormhole can be formed using, first, in-band channel packet to another malignant node m2 using encapsulation even though there is one

or more nodes between two malignant nodes, the nodes following m2 nodes believe that there is no node between m1 and m2 employ an physical channel between them by either dedicated wired link or long range wireless link shown in Figure 2.

When malignant nodes form a wormhole, they can disclose themselves or hide themselves in a routing path. The former is an exposed or open wormhole attack, while the latter is a hidden or close one.

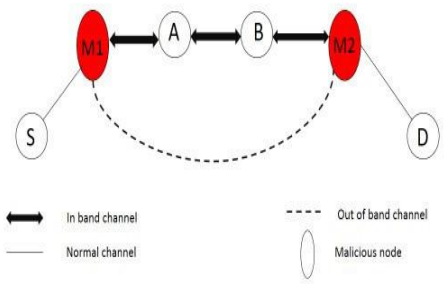


Figure 2: Wormhole Attack

IV. PROPOSED TRUSTED AD-HOC ON DEMAND DISTANCE VECTOR (TAODV)

In proposed method, we make some assumptions and establish the network model of TAODV to prevent wormhole attack in MANET.

Mobile nodes in MANETs often communicate with one another through an error-prone, bandwidth-limited, and insecure wireless channel. Our concern the security problem introduced by the instability of physical layer or link layer. We only assume that: (1) Each node in the network has the ability to recover all of its neighbors; (2) Each node in the network can broadcast some essential messages to its neighbors with high reliability; (3) Each node in the network possesses a unique ID, the physical network interface address for example, that can be distinguished from others.

In order to detect and prevent the wormhole nodes in the network the below technique used the concept of the bait destination node only. It works in the following way:

- ✓ First the source node will haphazardly pick one of its neighbors as the lure goal address.
- ✓ Now the source will communicate the lure route request in the entire system.

- ✓ Case 1. Considering the neighbor isn't the wormhole:

Source will have the answer from the neighbor itself whose address was utilized to send the snare route request. What's more, the source will likewise have an answer from the wormhole node that have made the passage in the network.

- ✓ Case 2. Considering the neighbor is the wormhole:

Right now, pair with which secure way has been made by the trap destination node will be found some place in the network. The source node will get just one answer however right now way to snare destination will be experiencing some other node.

- ✓ Since the node is one jump neighbor of the source node, so the answer must not have bounce include more prominent than one in both the cases. This implies the answer that originated from the nodes is bogus guaranteeing way to destination and having hope tally of more than one is bogus. What's more, source node will place the nodes in the presumed list.
- ✓ Now subsequent stage is to discover which nodes in the way are malignant nodes.
- ✓ For this the source node will send hardly any test parcels over the way and if the packet drops happen on any of the node, the source node will put that node just as the forerunner node in the pernicious node list.
- ✓ Source will currently send the first destination route request. Alongside route request, it will illuminate the nodes to not speak with the malignant nodes.
- ✓ Now the ordinary correspondence will continue over the new path. The new way won't contain any wormhole nodes in it.

V. IMPLEMENTATION & RESULTS

In this work Creation of MANET Scenario for NS-2 and then to create Different routing protocols with the use of various performance matrices Like Packet Delivery Ratio, Throughput, Residual Energy andEnd to End delay. In this work firstly created scenario file for IEEE 802.11 standard which has to be used along with TCL Script than we have created a TCL script consist of various routing protocols i.e. AODV, WAODV and TAODV than a particular MANET scenario or topology Network size is considered as 2000m X 2000m and the numbers of nodes are 10, 20, 30, 40and 50 nodes in the sensor field. Parameters for this simulation are as follows:

Simulation Tool	NS-2.35
IEEE Scenario	802.11
Propagation	Two Ray Ground
Network area	25, 50, 75, 100, 125, 150 nodes
Traffic Type	TCP
Antenna	Omni directional antenna
MAC Type	IEEE 802.11
Routing Protocol	AODV, WAODV, TAODV
Queue limit	50 Packets
Simulation area (in meter)	1000*1000
Queue type	Droptail
Channel	Wireless Channel
Simulation time	100 sec.

a. Packet Delivery Ratio

Packet delivery fraction is the ratio of the numbers of packets originated by the CBR sources to the number of packets received by the CBR sinks at the final destinations.

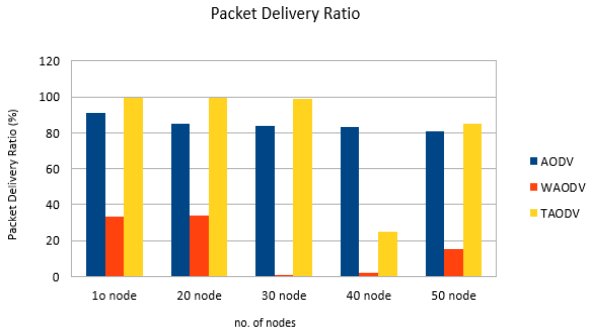


Figure 3: Packet Delivery Ratio

b. Throughput

The throughput of the protocols can be defined as percentage of the packets received by the destination among the packets sent by the source. The throughput is measured in kbps.

This simulation analysis is made from the graph sources. Here we analyze various parameters with respect to varying pause times.

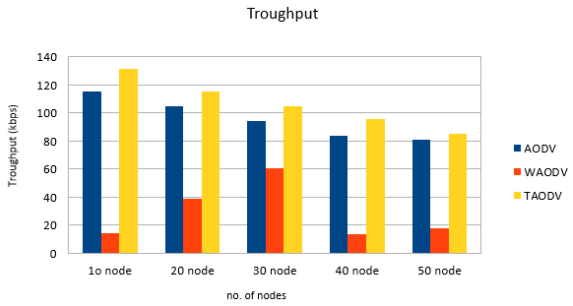


Figure 4: Throughput

c. Residual Energy

Total amount of energy used by the Nodes during the Communication or simulation, nodes having lower remaining energy are not participated at the time of communication, so the low energy nodes can be used during crucial condition in future.

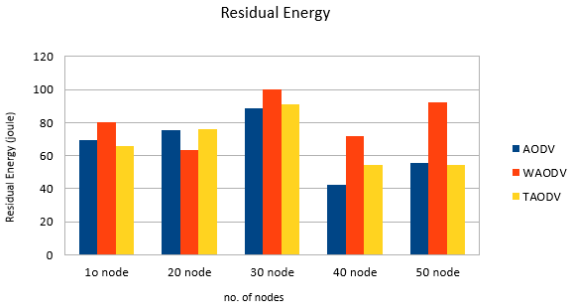


Figure 5: Residual Energy

d. Average End-to-End Delay

This includes delays caused by buffering of data packets during route discovery, queuing at the interface queue, retransmission delays at the MAC.

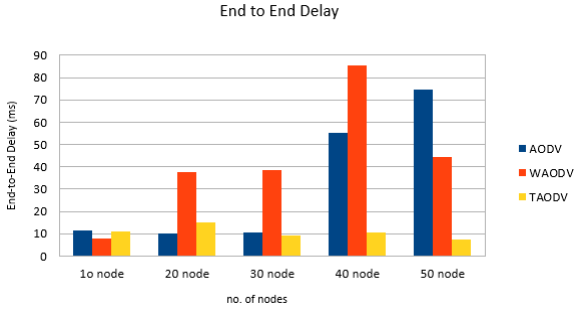


Figure 6: Average End to End Delay

VI. CONCLUSION

Proposed Trusted routing technique in which various node density-based scenarios are formation with optimization of our proposed Trusted routing technique in transmitting data to the leader was analysed and emphasized and analysis shows that service efficiency of MANETs is improved by

using the trust-based routing technique. The concept of trust-based routing technique can be effectively used to designed efficient routing protocol in MANET. With good quality of service awareness trusted protocol, our proposed trust-based routing technique uses the trust value algorithm to send data to the leader as proof to offer more reduced drop packets and also increase the lifetime of the network. From the analysis of this simulation results, it has been found that TAODV protocol offers a solution to prevent against wormhole attack usage in a MANET when compared to other routing protocol such as AODV.

REFERENCES

1. Corson, S., and Macker, J. "Mobile Ad hocNetworking (MANET): Routing ProtocolPerformance Issues and EvaluationConsiderations"RFC 2501, IETF, Jan. 1999.
2. Royer, E., and Toh, C. "A Review ofCurrent Routing Protocols for Ad HocMobile Wireless Networks" IEEE PersonalCommunications, 6(2), Apr. 1999, pp. 46–55.
3. V.VioletJuli and J. Arputha Vijaya Selvi, 2014."GeneticAlgorithm andtheir Tandem Application in Wireless Sensor Network Deployment"Research journal of Applied Sciences, Engineering andTechnology,8(24):2426-2438.
4. Gagandeep, Aashima and Pawan Kumar. 2012." Analysis of differentsecurity attacks in MANETs on protocol stack"Int. J. Engg. Adv.Technol. 1(5).
5. M.Soniya, P.Sabarinathan, S.Visnudharsini, 2014, "Enhancing Securityin Wireless Ad-Hoc Network Using ZKP," International Journal ofInnovative Research in Computer and Communication Engineering,Vol.2, Special Issue 1.
6. E.Hern´andez-Orallo,M. D. S. Olmos, J.-C.Cano, C. T. Calafate,and P. Manzoni, "CoCoWa: a collaborative contact-basedwatchdog for detecting selfish nodes," IEEE Transactions onMobile Computing, vol. 14, no. 6, pp. 1162–1175, 2015.
7. J. Biswas, A. Gupta, and D. Singh, "WADP: a wormhole attackdetection and prevention technique in MANET using modifiedAODVrouting protocol," 9th IEEE InternationalConference on Industrial and Information Systems (ICIIS'14), pp. 1–6, December 2014.
8. M. M. Patel and A. Aggarwal, "Two phase wormhole detectionapproach for dynamic wireless sensornetworks," IEEE International Conference on Wireless Communications,Signal Processing and Networking (WiSPNET '16), pp.2109–2112, Chennai, India, March 2016.
9. R. Matam and S. Tripathy, "WRSR: wormhole-resistant securerouting for wireless mesh networks," EURASIP Journal onWireless Communications and Networking, vol. 2013, article 180,2013.
10. Dhruvi Sharma, Vimal Kumar, Rakesh Kumar, "Prevention of Wormhole Attack Using Identity BasedSignature Scheme in MANET "ComputationalIntelligence in Data Mining. Volume 2. Volume 411of the series Advances in Intelligent Systems andComputing pp 475-485. 10 December 2015,Springer.
11. Rajan Patel, Anal Patel, Nimisha Patel, " Defending Against Wormhole Attack in MANET" Fifth International Conference on Communication Systems and Network Technologies, 2015 IEEE.
12. Ashish Kumar Jain, Ravindra Verma, " Trust-Based Solution For Wormhole Attacks In Mobile Ad Hoc Networks" Volume-4, Issue-12, November- 2015, Global Journal Of Multidisciplinary Studies.