ISSN:0975-9646

Effect of MANETS With and Without Malicious Node

Katroth Balakrishna Maruthiram
M.Tech – Computer Science
School of IT, JNTUH.

Sri.Kare.Suresh Babu
Assistant Professor
School of IT, JNTUH

Abstract: A MANET is a self configuring network of mobile devices connected by wireless links. well-organized routing is one of the key challenges of a mobile Ad Hoc network(MANET). Each device in the network is free to move in any path; therefore links with other devices change commonly. These networks do not have any permanent base stations. Hence each node should act as a router. In order to make easy communication within the network, a routing protocol is used to find out routes between nodes. The main goal of such an ad-hoc network routing protocol is accurate and efficient route organization among a pair of nodes so that messages may be delivered in a appropriate method.

Routing in Ad Hoc Networks has established a important consideration with a number of dissimilar routing protocols, like proactive, reactive and hybrid. normal routing protocols like DSR, DSDV, TORA and AODV which are the shortest path protocols for Ad Hoc networks. But all these routing protocols do have some compensation and disadvantage of their individual. Depending on the situation we can say which protocols works enhanced for that condition.

Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are insecure to attacks of the malicious nodes. Such attacks is the Black Hole Attack beside network integrity fascinating all data packets in the network. while the data packets do not arrive at the destination node on explanation of this attack, data loss will happen.

In this project, a complete challenge has been made to find the effect of malicious nodes on MANETS. we take a protocol say AODV and change it to identify the malicious nodes in the network. And then we evaluate the scenarios where how a manet works out malicious nodes and how it works with malicious nodes based on a little presentation metrics; for example No of dropped packets, throughput and packet delivery ratio. Simulation models and graphs are generated to give a clear demonstration and straight optical evaluation correspondingly, of the presentation of these protocols.

This is implemented in network simulator-2(ns-2). Ns is a separate event simulator under attack at networking research. Ns provides significant hold up for simulation of TCP, routing, and multicast protocols over TCP and UDP (local and satellite) networks.

Keywords: MANET, Routing Protocols, DSDV, TORA, DSR, DSR, AODV, NS2

I. INTRODUCTION:

MANET is a self configuring network of mobile devices connected by wireless links. Routing protocols are used for establishing a connection between source and destination nodes in the network. In this we describe the fundamental characteristics of a mobile ad-hoc network and the relevant routing protocols and about black hole attack.

Background and Existing Problems:

Mobile Ad hoc Network (MANET) is an independent method of mobile routers (and associated hosts) connected by wireless links - the union of which forms an random graph. The routers are free to move arbitrarily and arrange themselves randomly; therefore, the network's wireless topology may change quickly and suddenly. Such a network may work in a individual manner, or may be connected to the bigger Internet.

The power of the connection can modify quickly in time or even vanish totally. Nodes can become visible, vanish and re-appear as the time goes on and all the time, the network connections be supposed to work between the nodes that are part of it.

Ad hoc networks are not (necessarily) connected to any fixed (i.e. wired) transportation. An ad-hoc network is a LAN or other small network, with wireless connections, in which some of the network devices are part of the network only for the period of a communications gathering or while in close closeness to the have a break of the network.

In ad hoc networks every communication workstation (radio terminal RT) communicates with its colleague to carry out peer to peer communication. If the necessary RT is not a neighbor to the first calling RT (outside the coverage area of the RT), then the other middle RTs are used to carry out the communication link. This is called multi-hop peer to peer communication. This partnership between the RTs is very main in the ad hoc networks.

A Wireless ad-hoc network is a provisional network set up by wireless mobile computers (or nodes) stirring random in the places that have no network communications. Since the nodes be in touch with each other, they help by forwarding data packets to other nodes in the network. nodes find a path to the destination node using routing protocols. However, due to security issues, wireless ad-hoc networks are insecure to attacks of the malicious nodes.thus leads Black Hole Attack next to network reliability out of the normal all data packets in the network. because the data packets do not reach the destination node on relation of this attack, data loss will happen.

Problem Statement:

In NS2 as it is a simulator errors will not be there in any simulation. But in actual world errors will be generated in any operation of data. so we generate few errors (say malicious nodes) to know how these protocols work in real world and what is the network performance under the presence of malicious nodes. We need to evaluate a protocol which works on standard nodes and the same protocol how it works in case of malicious nodes in Mobile Ad-hoc Networks and by calibrating their performance in graphs for dissimilar parameters and to examine their performance over the unspecified situation.

Propose system: we compare these routing protocol in different scenarios by simulating the codes of these in ns2 and then based on the parameters like No.of dropped packets, throughput and packet delivery ratio we compare this routing protocol how it works with and without malicious nodes.

II. BACKGROUND AND RELATED WORK:

MANETs have special limitation and properties such as limited bandwidth and power, highly dynamic topology, high error rates etc., explained in the preceding sections. Moreover, compared to infrastructure based networks, in a MANET, all nodes are mobile and can be connected dynamically in an arbitrary manner. Nodes of MANET behave as router and take part in discovery and maintenance to establish a reliable route of each other. Therefore, routing protocols for wired networks cannot be directly used in wireless networks and numerous protocols have been developed for MANETs. Ad hoc Wireless network routing protocols can be classified into three major categories based on the routing information update mechanism. They are:

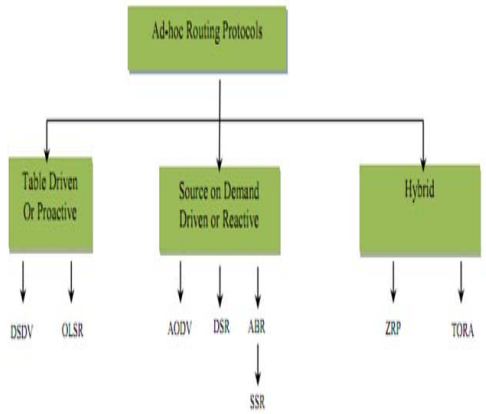

Fig-1: Classification of routing protocols in MANETS

A.Scope of the Paper:

Wireless ad-hoc networks are collected of independent nodes that are self- managed with no any communications. In this method, ad-hoc networks have active topology such that nodes can simply join or leave the network at any time. They have many possible applications, mainly, in military and rescue areas such as connecting soldiers on the battlefield or establishing network which indistinct past a calamity similar to an earthquake. Ad-hoc networks can set up a permanent infrastructure. because the nodes communicate with each other without an communications, they supply the connectivity by forwarding packets over themselves. To maintain this conned, nodes use routing protocols AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector).

further performing as a host, each node also acts as a router to find out a path and forward packets to the correct node in the network. As wireless ad-hoc networks not have an infrastructure, they are out in the open to a lot of attacks. One among them is Black Hole attack. In this malicious node absorbs all data packets in itself, related to a hole which sucks in all, all packets in the network are dropped. A malicious node reducing all the traffic in the network makes use of the vulnerabilities of the path finding packets of the on correct protocols, such as AODV. In route find process of AODV protocol, middle nodes are responsible to find a fresh path to the destination, sending discovery packets to the near nodes. Malicious nodes do not use this process and as an alternative, they directly respond to the source node with false information as though it has fresh sufficient path to the destination. thus source node sends its data packets through the malicious node to the destination assuming it is a right path. Black Hole attack could happen owing to a malicious node which is deliberately bad, as well as a injured node border. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node put away its battery.

In this paper, we simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. We made our simulations using NS-2 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the available network topologies. still while NS-2 contains wireless ad-hoc routing protocols, it will not have any modules to create malicious protocols. Thus, to suggest Black Hole attacks, we first added a new Black Hole protocol into the NS-2. We in progress our study by writing a new AODV protocol using C++,to simulate the Black Hole attack.

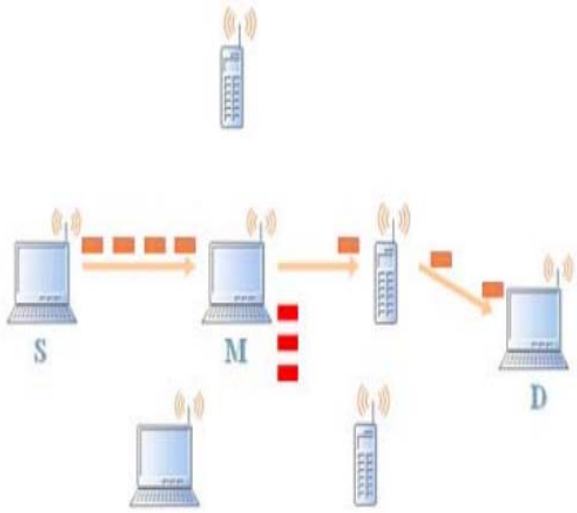

Fig-2: Scope of the Paper

III. ROUTING PROTOCOLS:

A. Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol:

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for finding a path to the destination in an ad-hoc network. To discover path to the destination all mobile nodes work in teamwork with the routing control messages. Thanks to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth use with small size control messages. The mainly unique feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route access. The destination sequence number is generated by the destination while a link is requested from it. by the destination sequence number ensures round self-determination AODV makes sure the route to the destination does not contain a loop and is the shortest path.

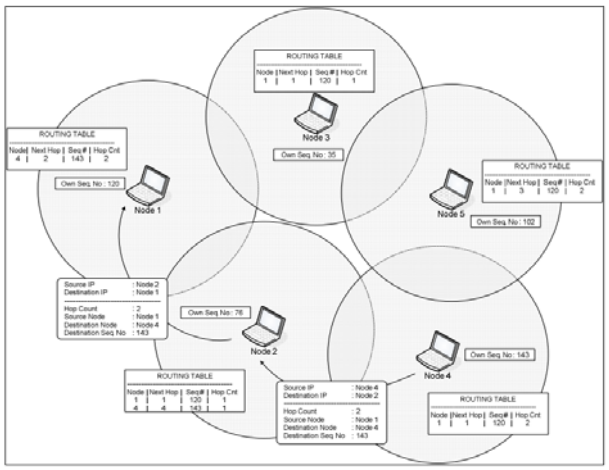

Fig-3: Unicasting the RREQ message

B.Sequence Numbers:

Sequence Numbers serve as time stamps and allow nodes to compare how fresh their information on the supplementary node is. though when a node sends any variety of routing manage message, RREQ, RREP, RERR etc., it increases its possess sequence number. Higher sequence number is other exact in sequence and any node sends the highest sequence number, its information is well thought-out and route is found greater than this node by the other nodes.

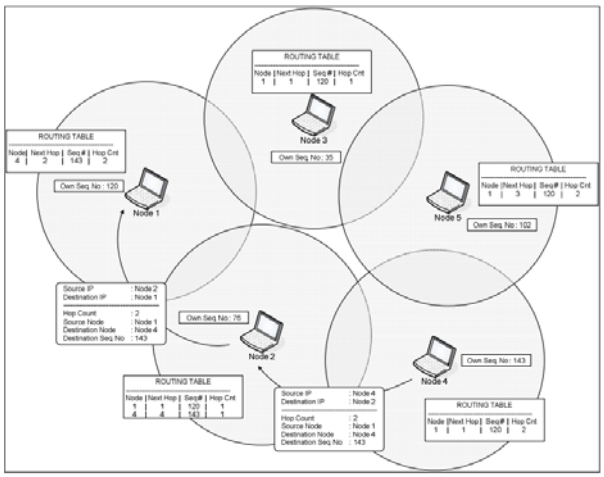

Fig.4: Updating the sequence number with fresh one

C.Black Hole Attack:

In an ad-hoc network with the purpose of uses the AODV protocol, a Black Hole node absorbs the network passage and drops all packets. To make clear the Black Hole Attack we added a malicious node that exhibits Black Hole performance in the scenario of the figures of the previous section.

In a Black Hole Attack, subsequent to a while, the sending node understands that there is a connection error since the receiving node does not send TCP ACK packets. To sends out new TCP data packets and discovers a new route for the destination, the malicious node at rest manages to deceive the sending node. If sending node sends out UDP data packets the problem is not detected since the UDP data connections do not wait for the ACK packets. In our scenarios we use UDP data packets.

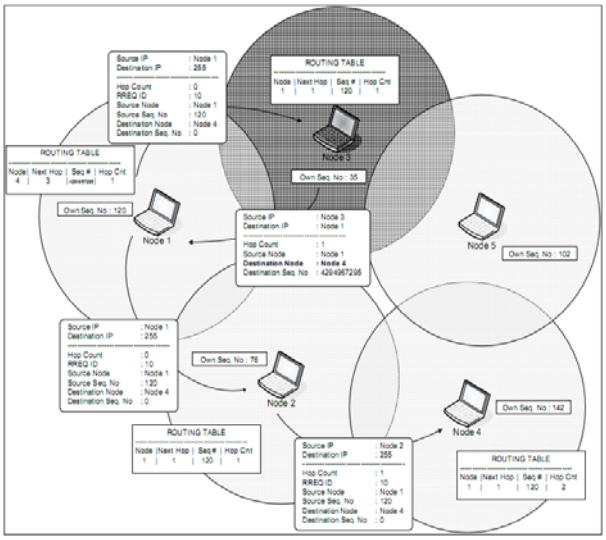

Fig.5: Illustration of Black Hole Attack

IV.CONCLUSION

This project compared the performance of AODV, DSR, and the network containing both AODV DSR,blackholeAODV routing protocols for ad hoc networks using ns-2 simulations. AODV,DSR, and the network containing both AODVDSR,blackholeAODV use the reactive on-demand routing strategy.

Among AODV,DSR,and the network containing both AODV DSR by varying Number of nodes and when simulation time is kept constant and the network containing both AODV DSR has higest performance than AODV and next DSR because as no. of nodes changes routes also changes. In AODV there is lifetime for routing table entries where as in DSR there is no lifetime for routing table entries. So AODV performs better than DSR. And in and the network containing both AODV DSR,AODV and the network containing both AODV DSR has more no of routing packets and throughput so the network containing both AODV DSR has better performance than AODV.

Among AODV,DSR,and the network containing both AODV DSR by varying simulation time and when number of nodes are kept constant DSR has highest performance then and the network containing both AODV DSR and next AODV because as simulation time is varying but no of nodes are kept constant same routing information will be same. In AODV there is lifetime for routing table entries where as in DSR there is no lifetime for routing table entries some time will be wasted in AODV due to these frequent updates. So DSR performs better than AODV. And the network containing both AODV DSR works better than AODV as the network containing both AODV DSR containins few nodes following DSR and few nodes following AODV, and the network containg both AODV DSR works better than AODV.

We have developed a new routing protocol with malicious nodes.In case of non cooperating nodes i.e AODV,blackholeAODV AODV performs better than blackholeAODV as blackholeAODV contains malicious nodes the no of dropped packets will be high its performance is low.

Final conclusion from the above simulations is:
Among the reactive protocols and the network containing both AODV DSR works better than AODV,DSR protocols.and among AODV,blackholeAODV AODV work better than blackholeAODV.

REFERENCES:

[1] Kapang Lego, Pranav Kumar Singh, Dipankar Sutradhar, "Comparative Study of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile Adhoc NETwork", Indian Journal of Computer Science and Engineering Vol. 1 No. 4 364-371, 2011.

[2] S.R. Birdar, Hiren H D Sarma, Kalpana Sharma, SubirKumar Sarkar , Puttamadappa C, Performance Comparison of Reactive Routing Protocols of MANETs using Group Mobility Model", International Conference on Signal Processing Systems, 2009.

[3] G. Jayakumar and G. Gopinath, "Performance comparison of two on-demand routing protocols for ad-hoc networks based on random way point mobility model," American Journal of Applied Sciences, vol. 5, no. 6, pp. 649-664, June 2008.

[4] S. Ahmed and M. S. Alam, "Performance Evaluation of important ad hoc networks protocols", EURASIP Journal on wireless Communications and networking, Vol: 2006, Article ID 78645, PP 1-11, 2006.

[5] Guntupalli Lakshmikant, A Gaiwak, P.D. Vyavahare, "Simulation Based Comparative Performance Analysis of Adhoc Routing Protocols", in proceedings of TENCON 2008.

[6] OLSR, internetdraft, http://tools.ietf.org/ html/draft-ietfmanet-olsr-00

[7] Rajiv Misra and C.R.Manda, ''Performance Comparison of AODV/DSR On-demand Routing Protocols for Ad Hoc Networks in Constrained Situation'', Indian Institute of Technology, Kharagpur (India).

[8] F. Bertocchi, P. Bergamo, G. Mazzini, M. Zorzi, ''Performance Comparison of Routing Protocols for Ad Hoc Networks'', DI, University of Ferrara, Italy

[9] H.D.Trung, W.Benjapolakul, P.M.Duc, "Performance evaluation and comparison of different ad hoc routing protocols", Department of Electrical Engineering, Chulalongkorn University, Bangkok, Thailand, May 2007

[10] J.Broch, D.A.Maltz, D.B.Johnson, Y-C.Hu, J.Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols", Computer Science Department, Carnegie Mellon University, Pittsburgh, USA. http://www.monarch.cs.cmu.edu/

[11] H.D.Trung, W.Benjapolakul, "Routing protocols in mobile ad hoc networks", in: Encyclopedia of Wireless and Mobile Communications, CRC Press, Book Chapter, in press.