International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-4, Issue-3, March 2016

Intelligent Node Route Detection Model for Secure Transmission in MANETS

Navpreet kaur, Pardeep kaur, Puneet Kumar

***Abstract*— A mobile ad-hoc network (MANET) is a major next generation wireless technology. Dynamically and arbitrarily located nodes communicate to each other to form a Mobile Ad-hoc Network. MANET is more susceptible to various types of attack than wired network. Black hole attack is more severe threat to MANET than any other attack. Prevention of Black hole attack is done by finding the malicious node before any harm can be done. Different techniques are proposed to prevent this type of attack. In this paper we proposed INRD techniques are studied with their advantages and disadvantages.**

***Index Terms*— MANET, AODV, RREQ, RREP**

I. INTRODUCTION

MANETs is an ad-hoc network which consists of number of mobile nodes [3], all nodes are interact with each other over wireless links [9]. Due to self-configuring ability, every node act as router as well as host in Manets [8][11]. If source node will send the data packet to destination then also use the intermediate nodes in the network. All mobile nodes are moves randomly & can leave or join the network [10]. MANETs are not uses any fixed infrastructure or centralized base station because it has dynamic topology [1].

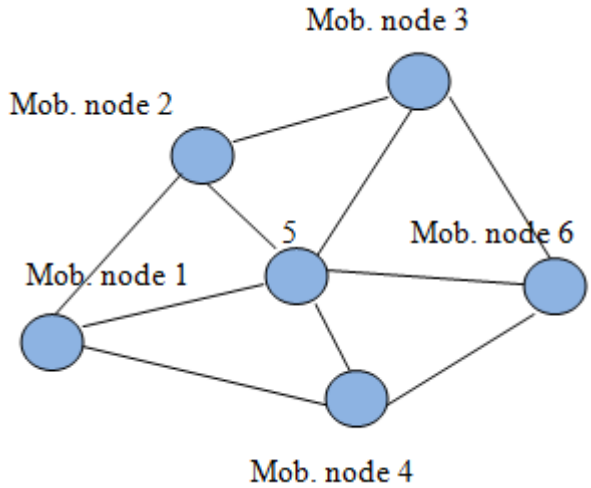


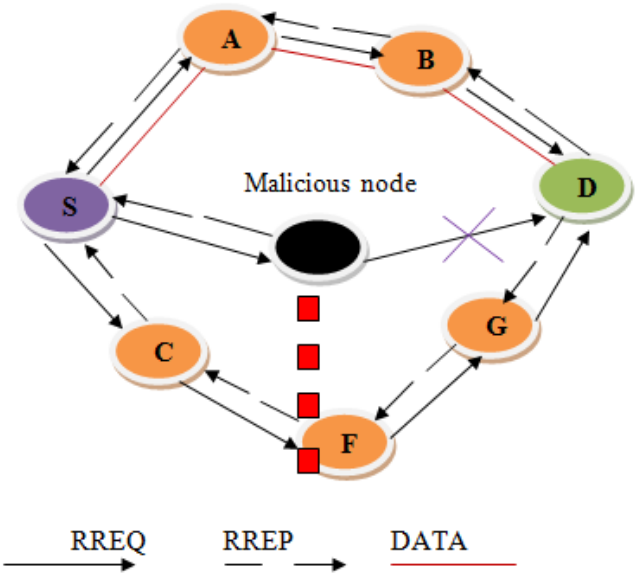
Fig.1 (Mobile ad-hoc network)

So Manets are mobile which use wireless connections to connect to various networks. These connections can be standard Wi-Fi connection or another medium [3]. Due to lack of mobility & resources, traditional protocol such as TCP/IP has limited use in Manets so this has lead to the development of many routing protocols such as AODV, DSR, TORA, MSR and ZRP.

II. BLACK HOLE ATTACK

Many routing threats also faces in Manets like black hole attack, wormhole attack, gray hole attack etc[13]. Black hole attack is considered as popular attack which belongs to DOS attack [11]. Black hole attack is defined in which malicious node provide fake path during routing process. When sender node sends the data packets to destination node, malicious node act as genuine node & broadcast fresh path to destination which interrupt the communication process because sender node sends all data packets to malicious node, so that malicious node take that packets sends other nodes not to destination node.[1][2]

In the network, if single malicious node is present which fails communication between sender & receiver node known as single black hole attack. On other hand, if two or more malicious node works together known as cooperative black hole attack.[12]



III. RELATED WORK

M.Sc.Ali Abdulrahman Mahmood, et al [1] proposed security technique to detect & isolate the malicious node which drops the data packets & disturbed the correct operation of the AODV routing protocol that cause black hole attack in the Manets. A proposed method used to find the secured routes by identifying the nodes with their sequence number, maintain the trust value for each node which helpful for prevents the black hole attack nodes in the Manets.

Tarek M.Mahmoud, et al [2] proposed Intrusion Avoidance system(IASAODV) can be considered as modification of the AODV protocol which can be used to detect & avoid the

Navpreet kaur, Student, M.Tech (CSE), PTU.

Pardeep kaur, Student, M.Tech (CSE), PTU.

Puneet Kumar, Assistant Professor, PTU

black hole attack in Manets. Using this proposed protocol as compared to AODV protocol gives better improvement in packet delivery ratio(PDR), throughput and
Normalized routing load (NRL) in the case of existing black hole attack.

Hitender Gupta, et al [3] introduced mechanism named RIP (restricted IP's) to detect and remove mainly two types of malicious nodes (black/gray hole) in ad-hoc network.

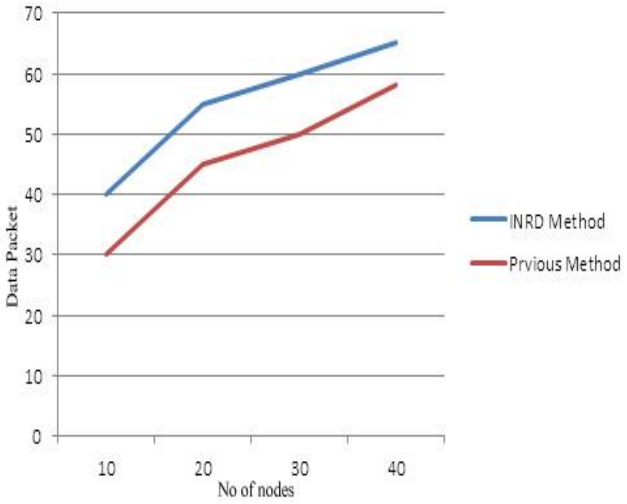
Swati Pokhariya, et al [4] proposed algorithm namely shielding algorithm which uses the shielding backbone node (SBBN) for detection and elimination of black hole/gray hole attack in Manets. Algorithm eliminates only the malicious nodes from the network which down the performances of network and gives better results.

Dilraj Singh, et al [5] proposed protocol Enhanced secure trusted (ESTA) AODV which is extension of broadly used reactive protocols used for prevention of black hole attack in Manets. The proposed protocol provides multiple path approach which means provides multiple paths are used for data communication. This multiple path approach combined with the use of trust to eliminate the corrupt paths.
Azza Mohammed et al [6] proposed a CROSSAODV method which is based on two process such as verification and validation for detection & removal of malicious node that cause black hole attack in AODV protocol. The verification process uses the RTS/CTS from which contains information about the requested path during the route discovery. The validation process consists of requesting the same information and comparing the requested routing information with the result of verification phase.
Alfy Augustine, et al [7] designed a watchdog mechanism basis of different intrusion detection system (IDS) to detect black hole node present in the network and generates an alarm message across the network. So that reception of the packet by the receiver is verified by sending an acknowledge packet back to source node.

IV. PROPOSED ALGORITHM

In the Proposed technique to detect the malicious node in network and Intelligent nodes are used for prevention and detection of black hole attack in the network In AODV the route request is send to neighbor nodes by the source node. If destination node is one of them then ok otherwise route request broadcast to next node until the destination is found. The route request (RREQ) packet header contains the information of visiting node (node id) in node information column and hop count column which contains the number of visiting nodes used in path. Using INRD path updated by these node will be used for prevention and detection proposed algorithm
Step 1: Generate Manet scenario using NS2
Step 2**:** Start with some initial elements like 'no of nodes', 'neighbor node', 'malicious node intelligent node
Step 3: Initialize with n no. of nodes.
Step 4: Implement INRD technique.
Step 5: initially Start INRD algorithm for finding malicious node in this process malicious node is detected
Step 6: In INRD the malicious node detected will be isolated from network and information regarding malicious node is broadcasted in the network
Step 7: Then finally With INRD Algorithm the secure network free from black hole will be formed
Step 8: This process continuation until the black hole is removed from network

V. RESULT AND ANALYSIS



The result show proposed INRD data transmission has better result than previous method

VI. CONCLUSION & FUTURE WORK

The proposed technique providing an efficient method that detects the malicious node in the network. Mobility is the main issue in network. Due to their dynamic nature, it will require higher security. The solution is implemented on 50 nodes. the future work of this is to remove the flooding problem.

REFERENCES

[1]. M.Sc.Ali Abdulrahman Mahmood, Dr. Taha Mohammed Hasan, M.Sc.Dhiyab Salman Ibrahim, "Modified AODV Routing Protocol to Detect the Black Hole Attack in MANET" International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume5, Issue7, July 2015
[2]. Tarek M.Mahmoud, Abdelmgeid A. Aly, Omar Makram M., "A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs" (IJCA), Volume 109 –No. 6, January 2015
[3]. Hitender Gupta,Harsh Aggarwal, "Simulation to Detect and Removal of Black Hole in Manet" SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) , ISSN:2348 -8549,April 2015
[4]. Swati Pokhariyal , Pradeep Kumar, "Shielding algorithm for Detection and Elimination of Black hole/Gray hole Attack in MANETs" International Journal of Modern Computer Science and Applications (IJMCSA), Volume No.3, Issue No.1, January 2015
[5]. Dilraj singh, Dr. Amardeep singh, "Multipath trust based framework for prevention of black hole attack in Manets" Journal of Theoretical and Applied Information Technology (JATIT & LLS), Vol.80. No.3, October 2015
[6]. Azza Mohammed, Boukli Hacene Sofiane and Faraoun kamel Mohamed, "A Cross Layerfor Detection and Ignoring Black Hole Attack in MANET" I.J. Computer Network and Information Security (IJCNIS), pg no. 42-49,Sept 2015

[7]. Alfy Augustine, Manju James, "Black Hole Detection using Watchdog" International Journal of Current Engineering and Technology, Vol.5, No.4 , Aug 2015
[8]. Rahul Patel, Maitrey Pate, "A Survey on Preventing DSR Protocol against Black Hole Attack for MANET" International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 09, Dec-2015
[9]. Payal Jain , Ashok Verma, Ashish Chaurasia, "Simulation Of Black Hole Attack Based On Varying Number Of Malicious Nodes In MANET Using NS-3" International Journal of Scientific Research and Engineering Studies (IJSRES),Volume 2,Issue12, December 2015
[10]. Ei Ei Khin, Thandar Phyu, "Impact of black hole attack on AODV routing protocol" International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014
[11]. B. Kondaiah, Dr.M. Nagendra, "A Black Hole Attack on Performance of AODV Routing Protocol in Manet" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 5, Issue 11, November 2015
[12]. Deepak Mishra, Mr. Srinivas Arukonda, "Black Hole Attack Prevention Techniques in MANET: A Review" International Journal Of Engineering And Computer Science, ISSN: 2319-7242, Volume 3, Issue 6, June, 2014
[13]. Nitesh Funde, P. R. Pardhi, "Analysis of Possible Attack on AODV Protocol in MANET" International Journal of Engineering Trends and Technology (IJETT),Volume11,Number 6 ,May 2014