International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-5, Issue-4, August 2016

A Proposed Method for the secure Transmission under Cooperative Blackhole Attack in MANETS

Manpreet kaur, Sandeep Kaushal

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— **AODV, MANET, RREQ, RREP.**

I. Introduction

A Mobile Ad hoc networks (MANET) are considered as promising communication networks in situations where rapid deployment and self-configuration is essential. In ad hoc networks, nodes are allowed to communicate with each other without any existing infrastructure. Typically every node should also play the role of a router and a host. This kind of networking can be applied to scenarios like conference room, disaster management, battle field communication and places where deployment of infrastructure is either difficult or costly.

Mobile Ad-hoc Network (MANET) is a self-configuring network of wireless and hence mobile devices that constitute a network capable of dynamically changing topology. The network nodes in a MANET, not only act as the ordinary network nodes but also as the routers for other peer devices [9]. The nodes themselves are responsible for creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed [10].There is no centralized gateway device to monitor the traffic within network. Since the medium is open for all nodes, both legitimate and malicious nodes can access it. Moreover, there is no clear separation between normal and unusual activities in mobile environment (false routing) can come from a compromised node or a legitimate node that has outdated information. [2]

Manpreet kaur, Department of ECE, ACET, Amritsar
Sandeep Kaushal, Associate Professor, Department of EEE, ACET, Amritsar

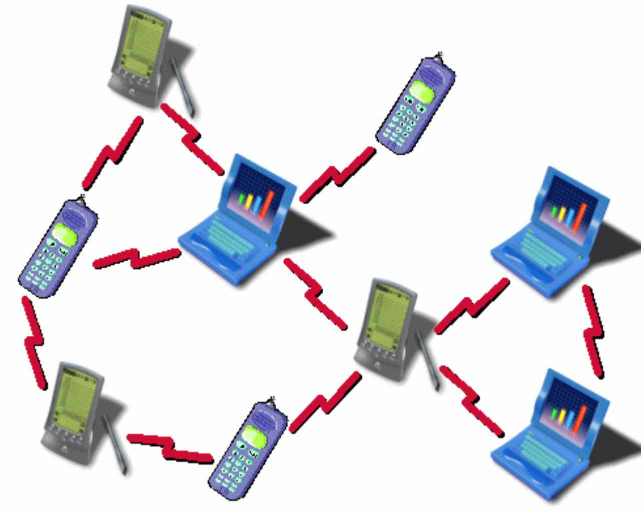


Fig1: Mobile Ad hoc Network [8]

II. Black Hole Attack

Many routing threats also faces in Manets like black hole attack, wormhole attack, gray hole attack etc [12]. 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]

Black hole attack is a routing layer attack in which data is revolves from other node. The transmission of packets on multiple nodes and dropping of packets is mostly occurring on routing layer. Routing protocol is besieged by the attack. Black hole attack has a great influence on virtual mesh network. The busy DOS attack is black hole attack. Black hole attack is difficult to detect; it is mostly found in temporary networks like virtual/wireless mesh networks. Black hole attack will cause powerful effect to the performance of mesh networks. In black hole attack, the sender node receive reply message from fault node and make smallest way to receiver node. Fault node sends reply message after authorized node to sender node which is then confused in two replies. On that way, fault node become sender node and whole data received by it. In this, the data packets fully dropped by sender node.[14]

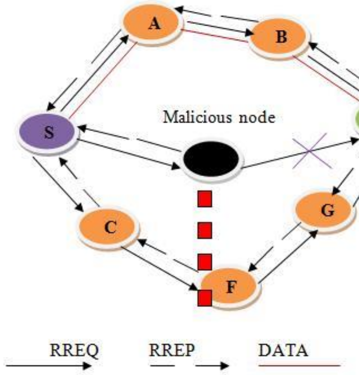


Fig.2 Black hole attack in Mobile ad- hoc network [12]

In Figure 2, the sender node S sends large amount of RREQ (route request) message to every nearby nodes. When RREQ message is received by fault node, then it sends RREP (route reply) message to sender node which is non-real and also shows the shortest way to reach to receiver node. Then the sender node accepts the reply message from non-real node which is called fault node and transfers the packets. This attack is known as black hole attack. Further, in black hole attack, a fault node accepted by sender node becomes a malicious node and all the data packets are dropped. This is also known as sleep deprivation attack.[13]

III. Cooperative Black Hole Attack

In Co-operative Black hole attack, more than one node combined mutually and act as Fake node is called as Cooperative Black hole attack [15]. This will affect the network performance than the Single Black hole attack. The Co-operative Black hole attack is shown in Fig.3.

Node S in figure 3 wants to communicate with the destination node D. The source node S broadcasts the Route Request (RREQ) packet. Each neighboring active node updates its routing table with an entry for the source node S, and checks if it is the destination node or whether it has the current route to the destination node. f an intermediate node does not have the current route to the destination node, it updates the RREQ packet by increasing the hop count.[15]

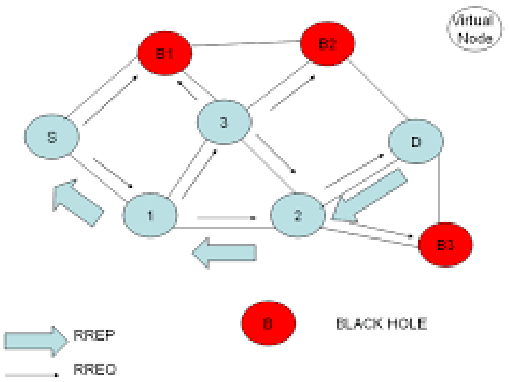
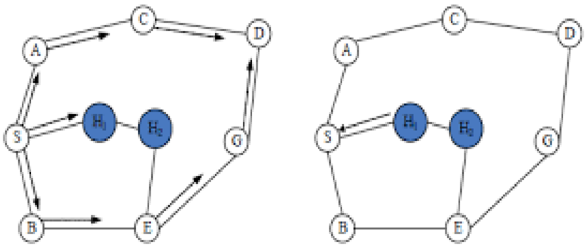


Fig3: Cooperative Black Hole Attack [17]

The network is flooded with the RREQ to the destination node D until it reaches node D or any other intermediate node that has the current route to D, as depicted in Figure 4.



(a) Network Flooding of RREQ (b) Propagation of RREP message

Fig4: Propagation of RREP messages [18]

The destination node D or any intermediate node that has the Current route to D, initiates a Route Reply (RREP) in the reverse direction, as depicted in Figure 4. Node S starts sending data packets to the neighboring node that responded first, and discards the other responses. This works fine when the network has no malicious nodes. However, the security threat arising out of the situation where multiple black hole nodes act in coordination has not been addressed. For example, when multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its partners B2. The source node sends a Further Request (FRq) to B2 through a different route other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D. Because B2 is cooperating with B1 its Further Reply (FRp) will be "yes" to both the questions. The destination node *D* or any intermediate node that has the current route to *D*, initiates a Route Reply (RREP) in the reverse direction, as depicted in Fig.4(b). Node *S* starts sending data packets to the neighbouring node that responded first, and discards the other responses. Thus, the packets are intercepted and then dropped by node B1.[16]

IV. RELATED WORK

Debarati Roy Choudhurya, et al [1] attempt to analyze the MANET's routing protocol and improve the security of viz. the Ad hoc On Demand Distance Vector (AODV) routing protocol. We propose modifications to the AODV protocol used in MANET an algorithm to reduce the Black hole attack on the routing protocols in MANETs. Wait time and Request Reply Tab table created to counter the Black hole attacks and the AODV protocol.

M.Sc.Ali Abdulrahman Mahmood, et al [2] 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 [3] proposed Intrusion Avoidance system(IASAODV) can be considered as modification of the AODV protocol which can be used to detect & avoid the 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 [4] 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 [5] 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 [6] 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 [7] 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 [8] 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.

V. PROPOSED ALGORITHM

In this system a heuristic Steadfastness technique will avoid multiple black holes acting in the group. The Technique is used to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. Our solution assumes that nodes are already authenticated and hence participate in communication. Assuming this condition, the black hole attack is discussed the approach is to Remove the Cooperative Black hole attack by the use of 'heuristic Steadfastness' where each participating node will be assigned a Steadfastness level that will be used to measure the of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and it is alerted by the node to its upstream and downstream neighbor node in each of the received RREP the Steadfastness level of the neighbor node, and each of its Next available hop's level are checked. If two or more routes seem to have the same Steadfastness level, then select the one with the least hop count; else, select the one with highest level.

Following are the steps of proposed algorithm:

Step 1: Generate Manet scenario using NS2 simulator

Step 2**:** Start with some initial elements like number of nodes, neighbor node, malicious node and an intelligent node

Step 3: In this step, the initialization is done. The system is initialized with n number of nodes.

Step 4: Implementation of HST (Heuristic Steadfastness Technique)

Step 5: initially Start HST algorithm for finding malicious node in this process malicious node is detected

Step 6: In HST the malicious node detected will be isolated from network and information regarding malicious node is broadcasted in the network

Step 7: Then finally With HST Algorithm the secure network free from black hole will be formed

Step 8: This process continuation until the black hole is removed from network

The given flow chart explains the working of Heuristic Steadfastness Technique. It shows the working of proposed algorithm.

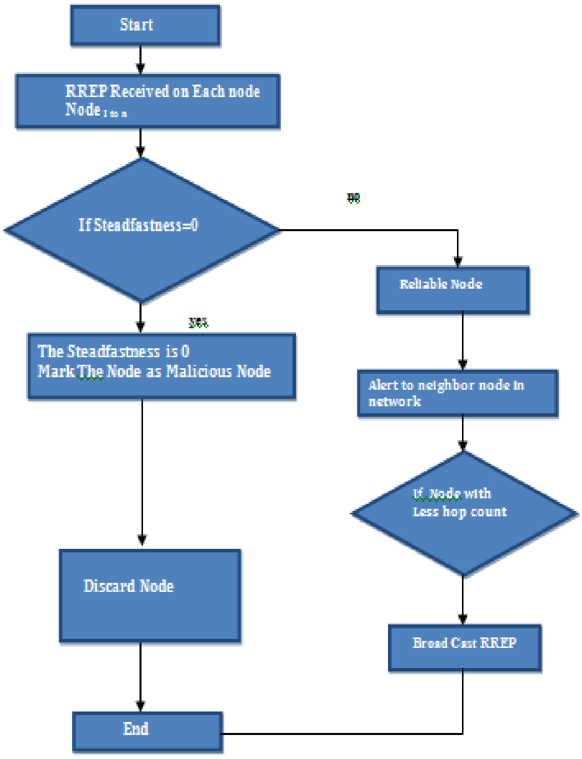

Start
RREP Received on Each node Node 1 to n
If Steadfastness=0
no
Reliable Node
yes
The Steadfastness is 0
Mark The Node as Malicious Node
Alert to neighbor node in network
If Node with Less hop count
Discard Node
Broad Cast RREP
End

Fig.5 The Working Flowchart for proposed technique

VI. CONCLUSION

In this paper, routing security issues in MANETs are discussed in general, and in particular the cooperative blackhole attack has been described in detail. A security protocol has been proposed that can be utilized to identify multiple blackhole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the blackhole nodes. The proposed scheme has been evaluated by implementing it in the network, shows the effectiveness of the mechanism. The solution is implemented on 50 nodes.

VII. FUTURE WORK

As a future scope of work, the proposed security mechanism may be extended so that it can defend against other attacks like resource consumption attack and packet dropping attack. Adapting the protocol for efficiently defending against grayhole attack- an attack False positives occur when the our proposed mechanism reports that a node is misbehaving when in fact it is not. We plan to study the impact of this on throughput. where some nodes switch their states from blackhole to honest intermittently and vice versa, is also an interesting future work.

REFERENCES

[1] Debarati Roy Choudhurya, Dr. Leena Raghab, Prof. Nilesh Marathe.b*,” Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack”, International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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

[8] Alfy Augustine, Manju James, “Black Hole Detection using Watchdog” International Journal of Current Engineering and Technology, Vol.5, No.4 , Aug 2015

[9] Sanjeev Jain Sudhir Agrawal and Sanjeev Sharma. “A survey of routing attacks and security measures in mobile ad-hoc networks” Journal of Computing, 2011.

[10] Robinpreet Kaur and Mritunjay Kumar Rai. A novel review on routing protocols in manets.Undergraduate Academic Research Journal, 1, 2012

[11] B.Kondaiah,Dr.MNagendra, “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] 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

[13] Vipan Chand Sharma “Detection of Black Hole Attack in MANET under AODV Routing Protocol” International journal of Advance computer science IJARCSE vol jan 2014

[14] Ms Suchaita b Patil ” An Evolution of Different Layered based Attacks and Security Actions for Blackhole attack in Mobile Ad Hoc Network” International Journal of Application Engineering & Management IJAIEM vol feb 2013

[15] G.Vennila “Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm” vol oct 2014

[16] Jaydip Sen1, Sripad Koilakonda2, Arijit Ukil3,” A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks”. Innovation Lab Tata Consultancy Services Ltd. Kolkata-700091, INDIA Email: {1jaydip.sen, 2sripad.k, 3arijit.ukil}@tcs.com

[17] Raja Karpaga Brinda .R, Chandrasekar.P, “Detection and Removal of Co-Operative Black Hole\Black Hole Attack in Manet”, International Journal of Computer Applications (0975 – 8887) Volume 43– No.11, April 2012

[18] Shree Om, Mohammad Talib, “ Using Merkle Tree to Mitigate Cooperative Black-hole Attack in Wireless Mesh Networks”, (IJACS International Journal of Advanced Computer Science and Applications, Vol. 2, No. 5, 2011