Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 08, August-2016

The Heuristic Steadfastness Approach to Enhance Performance under Cooperative Black Hole Attack in Manet

Manpreet Kaur
Department of ECE
ACET College, Amritsar

Sandeep Kaushal
Department of ECE
ACET College, Amritsar

***Abstract*— Security in mobile ad hoc network (MANET) is the most essential concern for the fundamental functionality of network. MANETs often suffer from diverse security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism. Though ad-hoc on demand Distance Vector (AODV) is one of the principal routing protocols yet it is exposed to the Black hole attacks, where a malicious node falsely advertises good paths to a destination node during the route discovery process. Such malicious nodes affect the network performance severely by dropping all the data packets instead of forwarding it to intended receiver. This attack becomes more severe when a group of malicious nodes work together with each other which results in "Co-Operative Black hole Attack" i.e. the nodes collude to each other hence, making this attack more challenging to identify. In this paper, we have enhanced AODV protocol with Heuristic Steadfastness Technique which will help to detect and eliminate co-operative blackhole attack from the network on the basis of intelligent route discovery.**

Keywords: AODV, HST, IRDN, Trust Factor

I . INTRODUCTION

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 [8]. 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in mobile environment false routing information can come from a compromised node or a legitimate node that has outdated information [10]. Due to this temporary topology and self-motivated mobile nature of the nodes, these are more exposed to security threats which disturb the performance of the network. The black hole and Cooperative black hole attacks are the chief security problems that occur in mobile ad hoc networks (MANETs). Major routing protocols are exposed to these well known attacks which are intended to hinder the working of the network. Moreover, in a MANET, there is no fixed infrastructure (Base Station) and since nodes are free to move, the network topology may dynamically change in an unpredictable manner. In this network, each node acts as a router and along with its usual job as common device. The organization of Ad hoc networks is peer-to-peer multi hop and information packets are relayed in a store-and-forward mode from a source to any arbitrary destination via intermediate nodes. As the nodes are mobile, any change in network topology must be communicated to other nodes so that the topology information can be updated or eliminated. It is not possible for all mobile nodes to be within the range of each other. However, all the nodes are close by within radio range [9].

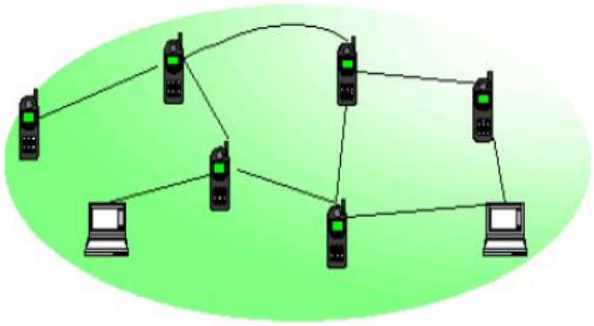

Figure 1: Infrastructure less networks [10]

Such an open medium, dynamic topology, distributed cooperation results in constrained capability.

II. DESIGN ISSUES/CHALLENGES IN MANETS

Temporary wireless networks have the conventional problems of wireless communications, such as power control, enhancing the quality of transmission, while, in addition, multi-hop nature, their mobility, and the lack of infrastructure causes many complexities and design constraints. Few of manet design issues are mentioned below:

Network Security: Mobile networks are more vulnerable to security threats than fixed-wired networks. Mobile networks are more vulnerable to security threats because it uses open and shared broadcast wireless channels means nodes with inadequate physical protection. In addition, because a mobile ad hoc network is an infrastructure-less network, since there is no centralized security control MANET mainly relies on individual security solution from each mobile node.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 08, August-2016

Robustness and Reliability: MANET is multi-hop network, so network connectivity is obtained by forwarding and routing among multiple nodes. Although MANET comes with the advantage of infrastructure-less, it also causes design challenges. Due to various types of failed links, a node may fail to forward the packet, like overload or acting selfishly. Unreliable links and misbehaving nodes and can have a severe impact on overall performance of the network. Such types of misbehaviours cannot be found and isolated quickly because of the lack of centralized monitoring and management mechanisms. This increases the design complexity significantly.

Energy Constrained Operation: Each node in MANET is battery powered which cannot be recharged. So if a node runs out of the energy then this may cause partitioning of network. Since each node has limited power, energy becomes main threats to the network lifetime. Additional energy is required to forward packets because each node is acting as both a router and an end system at the same time [12].

Quality of Service: For the successful communication of nodes in the network Quality of Service (QoS) guarantee is very much essential. The different QoS metrics includes packet loss, throughput, jitter, delay, and error rate [11].

Limited Link Bandwidth and Quality: Since the mobile nodes communicate to each other via wireless links, it causes bandwidth-constrained, error-prone, variable capacity, since wireless links have significantly lower capacity than wired links and, hence, it causes network congestion [11].

Dynamic Topology: The dynamically nature of ad hoc network causes to the formation of an unpredicted topology. This topology change causes dropping of packets, partitioning of the network and frequent changes in route [11].

III. COOPERATIVE BLACK HOLE ATTACK

Blackhole attack is one of the most common attacks in MANET. It is a kind of denial of service (Dos) occurs in the network layer of OSI model. In blackhole malicious node send fake information by claiming that it has a fresh route to the destination node and hence source nodes select the shortest path and go through this malicious node. When the malicious node receives packets it discards the packets.

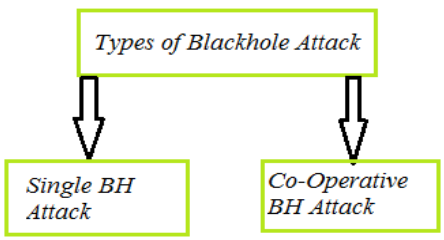

Figure 2: Types of Black Hole Attack

Hence, the data is lost that result in decreased packet delivery ratio and throughput. The single blackhole attack becomes more severe when it is Cooperative Black Hole attack.

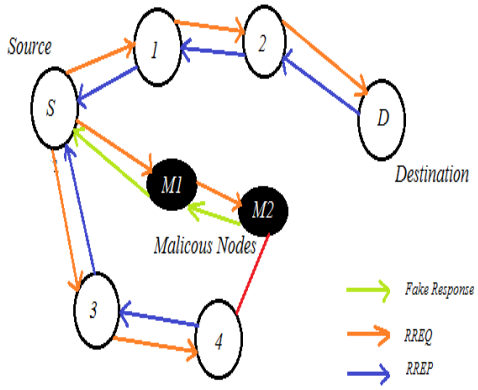

Figure 3: Cooperative Black Hole Attack

According to the original AODV protocol, when source node S wants to communicate with the destination node D, the source node S broadcasts the route request (RREQ) packet. The neighboring active nodes update their routing table with an entry for the source node S, and check if it is the destination node or has a fresh enough route to the destination node. If not, the intermediate node updates the RREQ (route request) (increasing the hop count) and floods the network with the RREQ to the destination node D until it reaches node D or any other intermediate node which has a fresh enough route to D. The destination node D or the intermediate node with a fresh enough route to D, initiates a route response (RREP) in the reverse direction. Thus, node S starts sending data packets to the neighboring node which responded first, and discards the other responses [13]. This works fine when the network has no malicious node one which claim itself as shortest path to destination without checking it's routing table for a fresh enough route to destination.

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. The author proposes modification 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.

P. V. Venkateswara Rao et al [2],simulated the Blackhole attack is in AODV using NS2 Simulator for both SANETS and MANETS by varying node density in the context of responsive and non-responsive traffic. From the simulation results, the impact of Black-hole attack on the performance of AODV QOS metrics i.e., throughput, packet delivery ratio is less, for end-to-end delay, routing load is high in MANET and SANET under responsive (TCP) and non-responsive traffic (UDP).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 08, August-2016

Anuj Ranaa et al [3] proposed that most demanding issue in MANETs is security or secure communication due to its various vulnerabilities. So an algorithm to prevent collaborative attacks on MANETs was presented. This algorithm is very much suitable for 15-45 nodes MANETs for preventing and detecting collaborative attacks black hole and gray hole. But little routing overhead in proposed EMAODV prevents full efficiency utilization of MANET which is not in case of normal AODV. Therefore routing overhead increases with increase in MANETs size.

Dr. S. K. Lenkac et al [4] has shown that a variable flooding nodes that floods the network for different time intervals have been evaluated using NS2 six different results are analyzed which shows drastic effect of such attack on QOS and throughput result also shows how packet delivery fraction is inversely proportion with bandwidth occupied by flood request.

Dr. Mohammed Ali Hussain, [5], considered only black hole attack. Black hole attack in MANETS is a serious security problem to be solved. Hence, the author provides a solution for countering black hole attack based on data routing information.

Dr.V.Egaiarasu et al, [6] proposed to design and instrument malicious node detection system to avoid black hole and worm hole attacks in MANETs. The author used Cooperative bait detection scheme to detect black hole attacks and to identify Worm hole attack as well a combined Performance Evaluation Multipath Algorithm in CBDS scheme.

Sunil Kumar Yadav et al, [7] are considering the blackhole attack on mobile ad hoc network. Here, proposed method is to detect and prevent cooperative blackhole attack in the MANET. Author modifies the existing DSR protocol to adopt the proposed cooperative algorithm of blackhole attack detection as well as prevention without the affecting overall performance of the network. Simulations for this work were carried out over the NS2 simulator.

V. PROPOSED WORK

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.

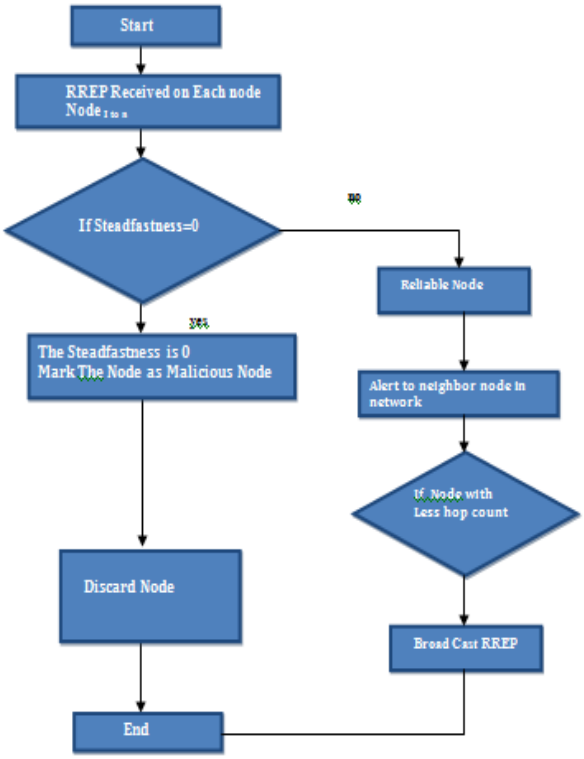

Fig.4 The Working Flowchart for proposed technique

VI.RESULT ANALYSIS

The figure 5 below show the comparitive graph of throughput results depending ujpon the network scenario which is after attack, previous technique and Heuristic Steadfasness technique. It is evident from the graph that results of proposed technique are better than other techniques for secure transmissions in a particular mobile adhoc network.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 08, August-2016

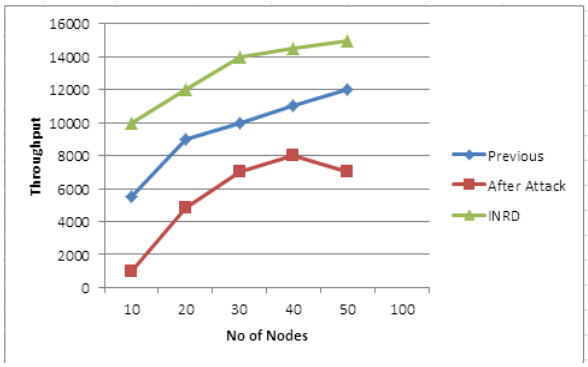

Figure.5 Comparison of resulting throughput

The figure 6 below show the comparitive graph of Packet Delivery Ratio results depending ujpon the network scenario which is after attack, previous technique and Heuristic Steadfasness technique. It is evident from the graph that results of proposed technique are better than other techniques for secure transmissions in a particular mobile adhoc network

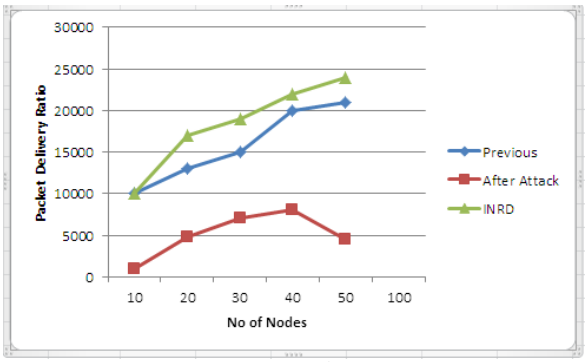

Figure.6 Comparison of resulting PDR

The figure 7 below show the comparitive graph of Packet Delivery Ratio results depending ujpon the network scenario which is after attack, previous technique and Heuristic Steadfasness technique. It is evident from the graph that results of proposed technique are better than other techniques for secure transmissions in a particular mobile adhoc network

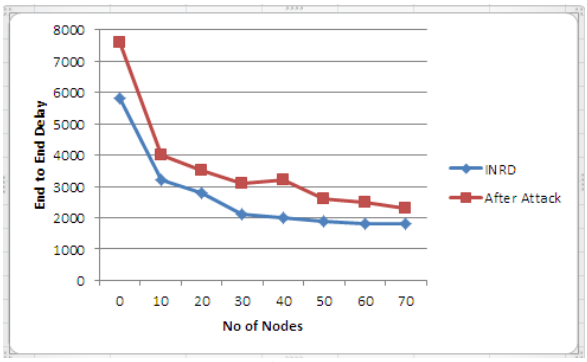

Figure.6 Comparison of resulting End to End Delay

VII.CONCLUSION

Black hole and cooperative are one of the serious threats in mobile ad hoc network. It affects the performance of the different routing protocol such as AODV by injecting a false route reply message and it also increases the network traffic. A study of different security mechanism has been proposed for the detection and prevention of such attack which have better packet delivery ratio and correct detection probability but have high overhead and end to end delay. A lot amount of work has been done to make the reactive routing protocol free from such threats but these methods do not avoid totally. So there is need for perfect prevention and detection mechanism. The heuristic steadfastness technique is proposed which has proved to be more advantageous than previous technique in detecting and removing the cooperative blackhole attack from the network for a secure transmission

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]. P. V. Venkateswara Rao, S. Pallam Setty, " Investigating the Impact of Black Hole Attack on AODV Routing Protocol in MANETS under Responsive and Non-Responsive Traffic", International Journal of Computer Applications (0975 – 8887) Volume 120 – No.22, June 2015

[3]. Anuj Ranaa,*, Vinay Ranab , Sandeep Gupta, "EMAODV: Technique To Prevent Collaborative Attacks In Manets" 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS, 2015[21]

[4]. Sourabh Singh Vermaa*, Dr. R. B. Patelb, Dr. S. K. Lenkac, "Investigating Variable Time Flood Request Impact Over QOS In MANET" Procedia Computer Science 57 (2015) 1036 – 1041, 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

[5]. S.J. Sultanuddin, Dr. Mohammed Ali Hussain, "An Efficient Approach for Countering Black Hole Attack in Manets", International Journal of Computer and Electronics Research [Volume 2, Issue 2, April 2013]

[6]. Dr.V.Egaiarasu, D.Kailashchandra, "Detection of Black Hole and Worm Whole Attacks in MANETS", SSRG International Journal of Mobile Computing & Application (SSRG-IJMCA) – volume 2 Issue 3 May to June 2015

[7]. Sunil Kumar Yadav, Shiv Om Tiwari, "An Efficient Approach for Prevention of Cooperative Black Hole Attack on DSR Protocol", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. V (Jan. 2014), PP 56-62

[8]. Vipan Chand Sharma,Atul Gupta, Vivek Dimri, "Detection of Black Hole Attack in MANET under AODV Routing Protocol", Volume 3, Issue 6, June 2013, ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering

[9]. Yujun, L.; Lincheng, H.;"The Research on an AODV-BRL to Increase Reliability and Reduce Routing Overhead in MANET," International Conference on Computer Applications and System Modeling (ICCASM 2010), IEEE, pp. 526-530, 2010.

[10]. 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, Volume 5, Issue 7, July 2015

[11]. Ashema Hasti, "Study of Impact of Mobile Ad – Hoc Networking and its Future Applications", BIJIT - BVICAM's International Journal of Information Technolog, December 2011

[12]. Gupta, P.; Gupta, S, "Performance Evaluation of Mobility Models on MANET Routing Protocols," Third International Conference on Advanced Computing & Communication Technologies, IEEE, 2013

[13]. Manita and Kapil Chawla, "A Survey on Various Attacks in MANET", IJCSMS (International Journal of Computer Science & Management Studies) Vol. 14, Issue 05, May 2014