Detection Of All Types Of Blackhole Attacks In MANET Using Fictitious Destination In Control Packet

Nitin Khanna
Assistant Professor, Department of Computer Science
Lyallpur Khalsa College, Jalandhar, India

Abstract- MANET is a network that is *infrastructure*-less and the nodes in this network can only communicate with farther nodes in multi-hop manner. The nodes possess the property of mobility and route is formed on ad-hoc basis as per requirements. Due to this characteristic nature of MANET, it is susceptible to many routing and security attacks. The most hazardous and common among those attacks is Blackhole attack which is a kind of packet drop attack. The variation of Blackhole attack also proves to be hazardous when executed intelligently. The variations of Blackhole attack like Grayhole attack and co-operative attack along with standard Blackhole attack becomes a bottleneck in the efficiency of secure MANET routing. In this paper, a mechanism is proposed that will mitigate the effect of all types of Blakchole attack and its variations. For it, a fictitious destination is used to make a trap for the malicious nodes and use of AODV routing protocol is made for accurate detection of Blackhole attack. This work is compared with published work EDRI (Extended Data Routing Information) and TLTB (Traffic Light Trust Based) mechanism against parameters like Packet Delivery Ratio, Normalized Control Load, Reliability of path formed and Accuracy of detection of attacking nodes in MATLAB 2017a environment.

Keywords- *AODV (Ad-hoc On-demand Distance Vector) Routing Protocol; Blackhole Attack; Bogus packet; Fictitious Destination; Route REQuest, Route REPly.*

I. INTRODUCTION

MANET stands for Mobile ad-hoc network that contains movable nodes that can move freely in any direction through a random movement model [38] or a designated movement model. The nodes in movement can show regular or irregular pattern depending upon the type of model used for movement. Due to ad-hoc nature the routes are formed according the requirement in a spontaneous way. Due to these intrinsic properties of MANET, this kind of network is prone to various security attacks like routing attacks, packet attack, data spoofing and other forms of security and service attacks. MANET is a decentralized [1] infrastructure-less network that has no central controlling system, so it paves the way for attacking nodes to disrupt the communication and various mechanisms has been devised for mitigation of different types of MANET security and routing attacks. For data routing in MANET different kind of routing protocols like DSR [9] (Dynamic Source Routing) protocol, AODV [10] (Ad-hoc On-demand Distance Vector) routing protocol, DSDV [20, 28] (Destination Sequenced Distance Vector) routing protocol, etc are used. These routing protocol are usually classified as re-active, pro-active or hybrid depending upon the mechanism used for route formation and maintenance. Re-active routing protocol [8] formulates the path only when it is needed and will not find the path even though it is so far never needed to formulate. Pro-active routing protocol [8] maintains all the routes all the time whether it is needed or not and thus causes the overhead of maintenance of paths that may never be needed while Hybrid routing protocol is a mixture of both re-active and pro-active schemes of routing in which at local level pro-active mechanism is used while for further nodes re-active mechanism is utilized.

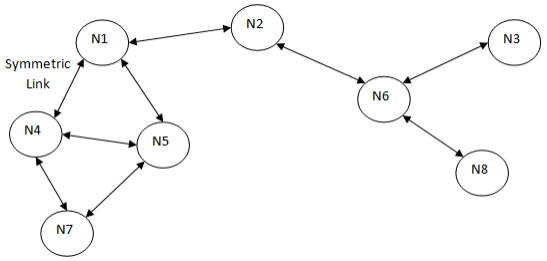

Fig.1: Mobile Ad-hoc NETwork

Pro-active routing protocols provide all the routes whether those are needed or not and thus cause overhead due to the effort wasted in establishing routes that might never be used. On the other hand, re-active routing protocols initiates the route discovery process only when the route is required and in this way causes minimal overhead of route maintenance of those routes that might never be needed but a delay [41] in route formation is involved in case a route that was not previously established but needed now. This happens when a source needs to communicate to a particular destination to which no other node has so far communicated and thus no path to that destination has been formulated and obviously high amount of packet overhead will be involved to establish a route to that particular destination. The choice of underlined routing protocol has effect on the mechanism that is employed for providing security against various attacks in the MANET and thus needs to be wisely chosen at the initial stage.

Packet drop attacks like Blackhole [6, 38], Grayhole [2] and co-operative Blackhole [21-22, 32, 39] are the most catastrophic attacks in MANET if not detected through the use of effective detection mechanism. Blackhole attack is a kind of attack in which the attacking node act as a Blackhole by replying with a fake RREP packet in response to a RREQ packet sent earlier by some source node, that RREP packet will have higher value of destination sequence number and relatively low hop-count value to convince the source node that it is the shortest and fresh most path to the particular destination. But actually it does not have any route to that destination and thus is just acting malicious looking for opportunity to hamper communication by dropping any data packets routing through it. When the source node sends data packets to that destination

through this Blackhole node that is acting as a legitimate intermediate hop, the Blackhole node drops each and every data packet to disrupt any communication between those two end nodes. This is the most basic and commonly executed packet drop attack but with great consequences that can prove to be very hazardous if no security mechanism [12] is deployed. Many mechanisms are researched and devised that can detect Blackhole attack in effective way but still it is a very serious and most common threat to the effective routing in MANET.

Grayhole attack, on the other hand, is a special kind of Blackhole attack in which the attacking node drops packets selectively and forwards the remaining and thus it is very difficult to detect this type of attack using mechanism devised for Blackhole attack detection. This packet drop attack is very rigorous as it is very difficult to formulate a mechanism that can accurately diversify a malicious attack from an unwilling collusion due to wireless link transmission that forms the basis of false positive. This attack is however, difficult to execute and complex in its true sense as it is driven by an artificial Intelligence or an intelligent adaptive program in the malicious node for continuous selection of packets that is to be dropped while forwarding others that appear as fair node to the other fair nodes in the network and does not come into notice if simple packet drop mechanisms are utilized.

Lastly, Co-operative Blackhole attack is a mega form of Blackhole attack in which two or more malicious nodes in coordination performs the packet dropping action. One node in the co-operation acts as forwarding node that reply with fake RREP packet to RREQ packet sent by source and when a data packet is sent through it, it forwards it to its malicious cooperative node that performs the packet dropping action. Thus both the nodes perform the packet dropping together attack without coming into notice to other nodes in the Network.

II. RELATED WORK

In this section, some published works are reviewed that come from various authors that provides solutions for detecting and mitigating packet drop attacks [11] and provide security to the communicated information from passive attacks. Watchdog [7] and Pathrater [7] are the mechanisms that are widely used for detecting Blackhole attack. Watchdog is used to detect Blackhole nodes by using a counter. This counter is maintained by every node in the network and it is incremented by node only if it does not overhear the forwarding of packet by next hop to a particular destination. If the counter reaches a predefined threshold, the next hop is marked as Blackhole and source node is notified. But standard Watchdog is not much accurate due to false positives and true negatives. Pathrater [7] mechanism is used to avoid forming routes that includes Blackhole nodes. This mechanism uses a rating method between 0 and 1 and Blackhole nodes are given -100 rating that is minimum of all. The reliability of path is calculated from the average of path rating of the nodes involved in the formation of that path. Thus, if the path involves a malicious node then its path rating would be very low and no such path is considered by the node. A wide variation of standard Watchdog mechanism is formulated by different authors for more accurate Blackhole detection. Bayesian Watchdog [13] and Kalman Watchdog [5] uses filters that will help in minutely detect Blackhole and avoid false positives and true negatives. These mechanisms use complex equation for calculating the reliability and trust level of nodes and nodes are considered malicious only if they yield a result below threshold after calculation through complex filter equations. These variation leads to high network overhead as a lot of data is transferred between all the nodes in the MANET. Multilevel Threshold Secret Sharing [16] and repository scheme [3] are solutions to the passive attacks and secure the information flowing through the network by the use of cryptography [12] and calligraphic techniques [15] that hides data from unintended intermediate nodes. These techniques provide good data security but puts high amount of load on the processor of mobile nodes. These techniques lead to high security overhead as they requires complex calculations at both ends that takes a lot of processing time and energy. Collaborative Watchdog [4] is also used for precisely detecting Blackhole attack and disseminates this information to other nodes in the network. This mechanism is based on the co-operation of various nodes in the network that shares the information about their neighbouring node and helps in disseminating information about malicious nodes. In this collaborative Watchdog, if the attacks go undetected, this will prove more problematic than the standard Watchdog. Watchdog-AODV [17] is a fast mechanism which collaborate Watchdog and AODV routing protocol and improves the route discovery. This mechanism on discovery of the malicious node, mark that node as Blackhole [11] and notify the source about the detection of a malicious node and route discovery mechanism is quickly initiated by the source. It suffers from similar drawbacks as of standard Watchdog mechanism. EDRI table [18] used in Grayhole detection and mitigation as it holds the Gray nature of malicious node. It uses further request and further reply [18] message to acquire gray nature of nodes. But it will create lots of load on the storage and processing of nodes and creates network overhead as well for acquiring gray nature of neighbourhood malicious nodes. This work from theoretic point of view is good but neglects the most important issue of power consumption is MANET. In [3], cryptography is used to enhance security of the routing protocol that provides greatest reliability but the handling of cryptography is very inefficient that leads to more power dissipation of nodes which is critical in MANET. Enhanced W-AODV [15] that includes various new fields provides better security but do not detect co-operative attacks. Trueness Level [14] helps in forming reliable routes in a more efficient way and proves to be excellent in connection with modified AODV routing protocol. Trueness Level [14, 25] provides a simple algorithm to generate a trust hierarchy and co-operation among fair nodes for malicious node detection and dissemination of such information.

CORIDS [24] tries to avoid Blackhole attack and detect when occur on the basis of cluster formation in which clusters performs the actual detection and routing process. Enhanced temporal windowing [26] performs cross-layer collaboration for detection of attacks by seeing the variation between RTS/CTS ratio with the actual packet delivery ratio. A threshold value [29] is used to confirm the variation as attack. EMLTrust [27] mechanism is based on the learning of the network to adapt to changing scenarios but requires high degree of complex algorithm. Anomaly based IDS [30] provide a windowed method for detecting the Blackhole attack by considering only the current behaviour of nodes. Co-operative mechanism [31] makes use of several packets for indication of sinkhole but causes a

lot of overhead. TRACEROUTE [33] mechanism uses the anomaly detection approach for breaking the co-operative attack collaboration by using trace and Reverse TRACE packets. Collaborative Bayesian Watchdog [18] makes uses of Bayesian filter for accurate detection of attacking nodes using inference. However, it also causes high degree of overheads in the network. LSAM [35] uses an acknowledgment based approach [36] that uses a sequence number based approach along with threshold value for any Blackhole attack or its variations detection. CBDS [37] uses a bait destination for accurate detection of Blackhole attack with the help of intrinsic property of DSR protocol.

III. AODV ROUTING PROTOCOL

Ad-hoc On-Demand Distance Vector Routing Protocol [23] is a re-active routing protocol in which route is formed as and when needed on demand. AODV uses four control packets; RREQ (Route REQuest), RREP (Route REPly), RERR (Route ERRor) and HELLO packets for establishing the routes and exchange information with neighbourhood and other nodes in the network about the reachability. It uses the concept of the sequence number and Broadcast-ID that will help in maintaining most fresh routes and avoiding the never ending flooding of route establishment packets. The maintenance of routing table is done at each node in such a way that all the intermediate nodes to the path store the next hop in the path to a particular destination with a desired high and valid sequence number. It uses broadcast-ID field in its packet which along with destination address forms a unique entry for the RREQ packet that help in keep a check on flooding of RREQ message during route discovery process. HELLO [23] messages are exchanged at regular interval by all the nodes with its neighbourhood to tell the other nodes in the network that are in its direct communication range about its reachability. The process of route discovery is explained through following figures:-

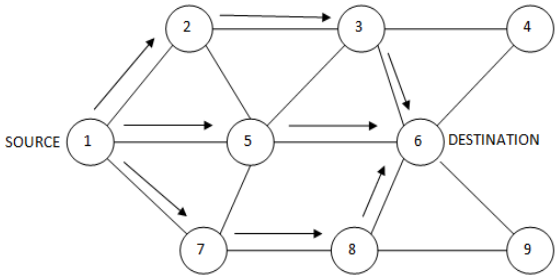

Fig.2: Route Discovery by Sending RREQ packet

In the figure above, source node 1 broadcasts RREQ packet to find a path to destination node 6 and on receiving the RREQ packet with destination 6, if any intermediate node has path to that node then it will respond with RREP packet, otherwise it re-broadcasts RREQ message by increasing the hop count by 1.

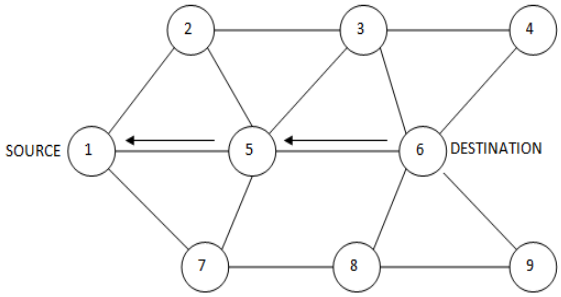

Fig.3: Destination Sending RREQ packet

On receiving RREQ packet, node 6 finds out that it is for itself and thus it responds with a unicasted [19, 40] RREP packet with its own destination sequence number. All the intermediate hops in the path update their routing table and unicasts the RREP packet towards the source node 1.

The header format for RREQ and RREP control packet of AODV routing protocol is given below:-

0-7	8-15	16-23	24-31
Type	Flags and Reserved Bits		Hop Count
Source IP Address			
Source Sequence Number			
Broadcast-ID			
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Origination Sequence Number			
Options			

Fig.4: Format of General RREQ packet [43]

0-7	8-15	16-23	24-31
Type	Flags and Reserved Bits		Hop Count
Source IP Address			
Source Sequence Number			
Broadcast-ID			
Destination IP Address			
Destination Sequence Number			
Options			

Fig.5: Format of General RREP packet [43]

IV. PROPOSED METHODOLOGY

In this section a Blackhole attack detection mechanism is presented that uses the traditional AODV routing protocol and its control packet to identify the attacking node. Firstly, as we know that a Blackhole node that is intended to perform packet dropping action will try to attract traffic through it by advertising itself as being having the most optimal and shortest route

in current situation and when the source sends a data packet to the destination through it, then it drops the packet and disrupt the communication. So, here a scheme called fictitious destination routing is presented in which a random fair node tries to find path to a bogus destination, i.e., a destination node that does not exist. Obviously, no other fair node has path to this fictitious node and will not reply with a path. Only the Blackhole node will respond with a fake path and when the source node finds out the RREP packet is received for a fictitious RREQ packet then it marks that as Blackhole.

Here to start with, the source node that wants to detect a Blackhole node in the network in its communication range will initiate the procedure by broadcasting a RREQ packet that involves a fictitious destination that does not exists in the network. This RREQ packet is no different from a regular RREQ packet except the fact that it contains request for the route to a destination that does not exists and that too is only known to the originator of this RREQ packet. The broadcast-ID for this packet is stored for further verification of received RREP packet. All the nodes that are non-attacking fair nodes on receiving this fictitious packet will forward it to their respective neighbourhood by just changing the hop count field. Only the active Blackhole node on receiving this RREQ packet will reply with a RREP packet that contains a fake hop count and a high value of destination sequence number to ensure source node that it has the shortest and most fresh path to the desired destination node. The Blackhole node which is generating this RREP packet has to include its own IP address and sequence number so that source can identify generator of RREP packet. So, when the RREP packet received by the source node then it checks the broadcast-ID of the RREP packet first, if that ID matches with any of the stored broadcast-ID [43] that is used for fictitious destination then the originator of the packet is marked as Blackhole and the information is disseminated in the entire network.

To elucidate the methodology, here a scenario is considered in which there are 10 nodes in the network with one Blackhole node as shown in the following figure:-

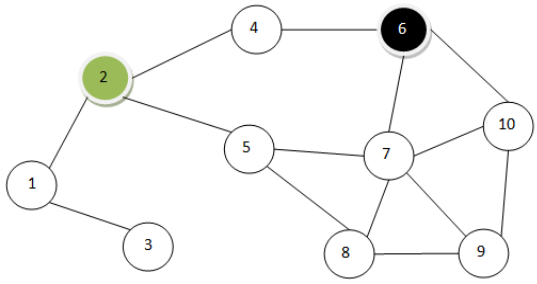

Fig.6: Illustration of Fictitious node tackling Blackhole Attack

In the figure above node 6 is the Blackhole node while node 2 is the node that initiates the detection process by assuming a fictitious destination that does not exists and tries to find a path to that destination. It generates a RREQ packet and broadcast it in the network and maintains the broadcast-ID of that RREQ packet in the list. All other fair nodes in the network like Node 1, Node 4 and node 5 will not have route to this fictitious destination so they re-broadcast it to their neighbourhood. When ultimately this RREQ packet reaches node 6 which is a Blackhole node, then it generates a fake RREP packet with some false hop count and redirect it towards the source node 2 with its IP address and sequence number in respective fields of RREP packet. On receiving the RREP packet generated by Blackhole node 6, node 2 checks the broadcast-ID of RREP packet and matches it with stored value in the list. If there is a match then source node 2 understands that it was for the purpose of detection and the destination does not exists and if there is any RREP packet coming in response to that then it must be coming from an attacking Blakchole node. Hence node 2 marks node 6 as Blackhole and disseminate the detection information to the other nodes in the network.

V. SIMULATION ENVIRONMENT

All the simulations and critical analysis of outcome is done in MATLAB 2017a environment. The proposed work fictitious node has been compared with the published work Extended Data Routing Table [34] (EDRI) and Traffic Light Trust Based (TLTB) [42] mechanism. All the source nodes in the network send 512 byte sized data packets excluding the header of packet. The simulation is done under static environment in which some parameters are fixed and some parameters of environment are varied to generate multiple scenarios. The assumed environment and parameters used for simulation of proposed work are described in the table below:-

TABLE 1: SIMULATION ENVIRONMENT AND PARAMETERS

PARAMETER	VALUE
NUMBER OF NODES	20,30,40,50
SPEED OF NODES (m/sec)	5, 10, 15, 20 m/Sec
ANTENNA TYPE	OMNI-DIRECTIONAL
% OF BLACK HOLES	10%
AREA	2000m X 2000m
NEIGHBOUR TIME	1s
SCENARIOS	8
WIRELESS INTERFACE	802.11
ROUTING PROTOCOL	Enhanced W-AODV
% OF BLACKHOLES	5-20 %
TRANSMISSION RANGE	250m
TRANSPORT PROTOCOL	TCP
MOBILITY MODEL	RANDOM WAY POINT

Various simulation scenarios are made by assuming a change in mobility speed, density of nodes that is defined by number of nodes in the network and the aim of scenarios is to provide in depth analysis of proposed work against published work for detection of Blackhole attack and its variants.

VI. RESULT AND DISCUSSION

In the experimental simulation, the proposed work fictitious destination has been evaluated against three parameters; Packet Delivery Ratio, Accuracy in detection of Blackhole and its variants and Normalized Control Load. The results for the proposed work for these parameters are then compared with the published work Extended Data Routing Information (EDRI) [34] mechanism and Traffic Light Trust Based Mechanism (TLTB) [42]. After comparison, the resulting graphs are then discussed to explain the impact of the proposed approach in AODV routing protocol usage in vulnerable MANET network. The results are calculated by varying both density of attacking Blackhole nodes, node density in the network and

mobilise speed of nodes. The network parameters are compared in graphical form with varying node mobility that comes to a numeral figure through averaging the values of other parameters at different node densities and attacking Blackhole densities, i.e., by changing number of nodes in the network along with changing the number of Blackhole nodes and keeping node mobility constant for that time. The result on the basis of different network parameters are shown and argued as follow: -

A. Packet Delivery Ratio (PDR) v/s Node Mobility

Packet Delivery Ratio is calculated through the ratio of total number of packets received by desired destination node and the total number of packets generated at the source node for that desired destination node. The higher the Packet Delivery Ratio in the network any instance, higher will be the efficiency and effectiveness of the network at same instance. It needs to be on the higher side always at any node mobility speed and even in presence of any kind of attacking nodes in any number to make the mechanism looks effective in its process and advantageous for the user.

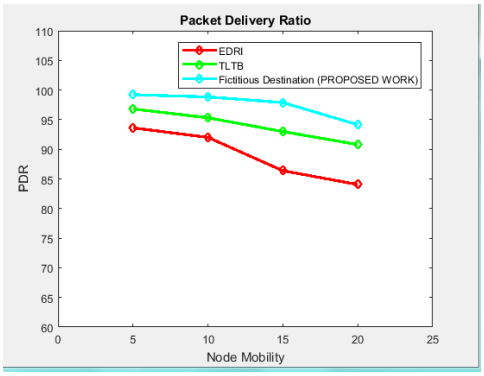

Fig.7: Packet Delivery Ratio Comparison between proposed and published works

In the figure above, through comparison of the proposed work with EDRI and TLTB mechanism, it is clearly visible that varying the mobility speed along with other parameters like node and Blackhole node densities will not affect much even at higher degree of mobility. The PDR level stays above 95% even at the hioghest 20 m/second mobility speed while the other two published work shows a declined in PDR at high speed. This is due to the fact that the Blackhole node detection process does not depend upon the routing pattern. It is solely based on fake destination to trap the attacking node and hence does not show much variation at high speed. The only decline in PDR is only to the fact that path are broken sooner at high mobility speed if the movement pattern is not well designed.

B. Normalized Control Load v/s Node Mobility

Normalized Control Load can be calculated as the ratio of total number of Control Packets generated by nodes in the network for route generation and maintenance and the total number of Data Packets received by the desired destination nodes and positively acknowledged. Normalized Control Load should be at lower side. However, it is bound to increase with high degree of mobility speed and if the node density is not increased along with that in greater proportion. This happens due to the fact that at higher mobility the path got disrupted relatively quickly due to breaking up of links between some neighbouring nodes.

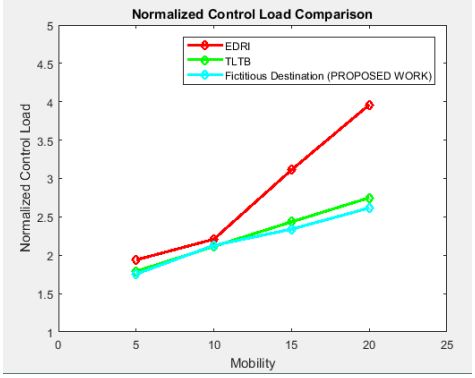

Fig.8: Normalized Control Load Comparison

From the comparison in above figure, it is clearly visible that the proposed work provides lower normalized control load at relatively higher degree of mobility speed and the mobility speed pattern has very little impact on it and that to only due to disruption of links between neighbourhood and not due to sending multiple control packets for detection of attack in network. While for other published work, the impact on control load is due to disruption of route as well as catastrophic effect of malicious activities of Blackhole nodes that go undetected due to higher mobility rates.

C. Accuracy in Packet Drop Attack Detection v/s Node Mobility

Accuracy in detection of Blackhole attack and its variants is calculated by computing the ratio between total number of attacking nodes discovered by the mechanism and the total number of attacking nodes actually exists in the network. As the accuracy rate is measured in percentage thus the ratio result is multiplied by 100 to get the final accuracy rate. The mechanism employed needs to be highly accurate to be of suitable and usable in actual MANET environment that is obviously prone to very malicious attacks like Blackhole and its variants.

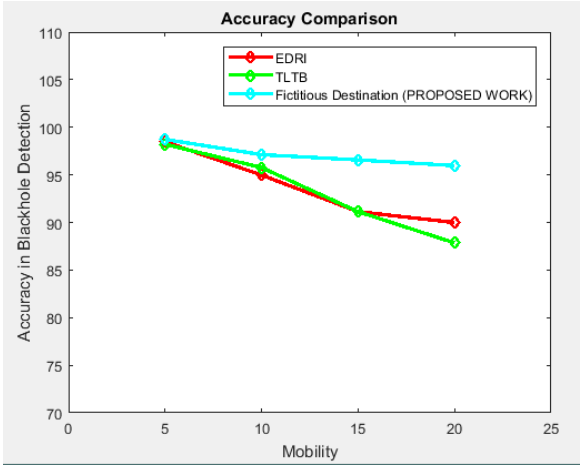

Fig.9: Accuracy in Packet Drop Attack Detection Comparison

As it clear from the comparison in above figure, that proposed mechanism is highly accurate even at varying mobility speed in any scenario and shows a very steep decrease at higher value of mobile speed. On the other hand, rest of the compared published work shows greater decrease in accuracy due to false positive and true negatives that has major impact at high mobility speed. The proposed work is free from false positive and true negative and as it is only dependent upon a fictitious destination and a fake RREP packet reception from attacking node that does not depend upon the mobile speed. Thus the mechanism is highly accurate. The small steep in accuracy at high mobility rate is due to the fact of dropping of fake RREP or RREQ packet for fictitious destination at high speed of mobility.

VII. CONCLUSION

Packet drop attacks such as Blackhole attack and all its variants can prove to be very hazardous if not handled in their inception state. So, this issue needs to be managed and sorted out through a detection or mitigation mechanism in a very effective and efficient manner. The mechanism proposed in this paper helps in identifying and eliminating all types of variants of Blackhole attack that too without hampering the smooth communication and increasing the overhead on the network. The mechanism makes use of fictitious destination that does not exists and detective node waits for the fake RREP packet from the attacking node and then mark it as malicious and disseminate the information in the entire network. The detection does not involve high calculation or extra burden on processors or network equipments and has is almost free from computational and network overheads. The accuracy is also of higher degree for the same reason as the mechanism can work well at any mobility speed that too with least control overhead.

As future work, it is proposed to enhance the mechanism to make the dissemination of information free from fake detection report without increasing the network and computational overhead. In addition to that a special routing attack, Wormhole attack [1] can also be considered for its mitigation.

VIII. REFERENCES

[1]. Punya Peethambaran and Dr. Jayasudha J. S., ―SURVEY OF MANET MISBEHAVIOUR DETECTION APPROACHES‖, International Journal of Network Security & Its Applications, Vol.6, No. 3, May 2014.

[2]. Gaurav, Naresh Sharma Himanshu Tyagi, ―An Approach: False Node Detection Algorithm in Cluster Based MANET‖, International Journal of Advanced Research in Computer Science and Software Engineering Vol. 4, No. 2, February 2014.

[3]. K. Sahadevaiah, Prasad Reddy P.V.G.D., ―Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks‖, MacroThink Institute, Vol. 3, No. 4, 2011.

[4]. Enrique Hernández-Orallo, Manuel D. Serrat, Olmos Juan-Carlos, Cano Carlos, T Calafate, Pietro Manzoni, ―A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs‖, Springer , August 2013.

[5]. Tushar Sharma, Mayank Tiwari, Prateek kumar Sharma, Manish Swaroop, Pankaj Sharma, ―An Improved Watchdog Intrusion Detection Systems In Manet‖, International Journal of Engineering Research & Technology, Vol. 2, No. 3, March 2013.

[6]. Vrutik Shah, Nilesh Modi ―An inquisition based Detection and Mitigating Techniques of AODV Protocol in Existence of Packet Drop Attacks‖, International Journal of Computer Applications, Vol. 69, No.7, May 2013.

[7]. D.Anitha, Dr.M.Punithavalli ―A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS‖, IJCSMC, Vol. 2, No. 3, pp. 112 – 119, March 2013.

[8]. Carlos de Morais cordeiro and Dharma P. Aggarwal, ―Mobile Ad-hoc Networking‖, 2004.

[9]. Andreas Tonnesen ―Mobile Ad-hoc Networks‖, 2004.

[10]. Charles E Perkins Elizabeth M Royer ―Ad hoc On Demand Distance Vector Routing‖, 1999.

[11]. Rashid Hafeez Khokhar Md Asri Ngadi Satria Mandala ―A Review of Current Routing Attacks in Mobile Ad Hoc Networks‖, 2008.

[12]. Behrouz A Forouzan ―Data Communications and Networking 4th Edition‖, Tata McGraw Hill Companies, 2004.

[13]. Serrat-Olmos, M.D. Hernandez-Orallo, E. ; Cano, J., Calafate, C.T., Manzoni, P., ―Accurate detection of black holes in MANETs using collaborative bayesian watchdogs‖, Wireless Days(WD), IEEE Conference, pp. 1-6, Nov. 2012. [14] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM 21 vol. 2, pp. 120–126, 2013.

[14]. Nitin Khanna, Parminder Singh, ―Mitigating Blackhole and Security attacks in MANET using Enhanced W-AODV with Trueness Level and Cryptography‖, IJRECE, vol. 3, no. 2, pp. 146-151, 2015.

[15]. Lein Harn Miao Fuyou, ―Multilevel threshold secret sharing based on the Chinese Remainder Theorem‖, Information Processing Letters 114, ELSEVIER, pp. 504–509, 2014.

[16]. Tarun Varshney, Tushar Sharmaa, Pankaj Sharma (2014), ―Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network‖, IEEE International Conference on Communication Systems and Network Technologies, pp. 217-221, June, 2014.

[17]. Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal,‖Detection and Removal of Co-operative Blackhole and Grayhole attacks in MANET‖, International Conference on System Engineering and Technology, Bandung, Indonesia, September, 2012.

[18]. M. D. Serrat-Olmos, "A collaborative bayesian watchdog for detecting black holes in MANETs", Intelligent Distributed Computing VI. Springer, (2013), pp. 221-230.

[19]. C. Panos and C. Ntantogian, "Analyzing, Quantifying and Detecting the Blackhole attack in Infrastructure-less Networks", Computer Networks, vol. 113, (2017), pp. 94-110.

[20]. S. Gurung and S. Chauhan, "A dynamic threshold based approach for mitigating black-hole attack in MANET", Wireless Networks, (2016), pp. 1-15.

[21]. U. Venkanna, J. Krishna Agarwal and R. Leela Velusamy, "A cooperative routing for MANET based on distributed trust and energy management", Wireless Personal Communications, vol. 81, issue 3, (2015), pp. 961-979.

[22]. B. Sharma, "a distributive cooperative approach to detect grayhole attack in manet", Proceedings of the Third International Symposium on Women in Computing and Informatics, ACM, (2015).

[23]. R. Hinge and J. Dubey, "Opinion based trusted AODV routing protocol for MANET", Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, ACM, (2016).

[24]. N. Deb, M. Chakraborty and N. Chaki, "CORIDS: a cluster-oriented reward- based intrusion detection system for wireless mesh networks", Security and Communication Networks, vol. 7, issue 3, (2014), pp. 532-543.

[25]. N. Khanna, "Avoidance and Mitigation of All Packet Drop Attacks in MANET using Enhanced AODV with Cryptography", International Journal of Computer Network and Information Security vol. 8, issue 4, (2016), pp. 37-43.

[26]. L. Sánchez-Casado, "A model of data forwarding in MANETs for lightweight detection of malicious packet dropping", Computer Networks, vol. 8, issue 7, (2015), pp. 44-58.

[27]. R. Akbani, T. Korkmaz b and G.V. Raju, "EMLTrust: An enhanced Machine Learning based Reputation System for MANETs", Ad Hoc Networks, Elsevier, Vol. 10, Issue 3, (2012), pp. 435-457.

[28]. A.A. Chavan, D. S. Kurul andd P. U. Dere, "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack", 7th International Conference on Communication, Computing and Virtualization, Procedia Computer Science, Elsevier, vol. 79, (2016), pp. 835-844.
[29]. A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha, "Threshold-based intrusion detection in ad hoc networks and secure AODV", Ad Hoc Networks, Elsevier, vol. 6, Issue 4, (2008), pp. 578-599.
[30]. L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro and R. Magán-Carrión, "A model of data forwarding in MANETs for lightweight detection of malicious packet dropping", Computer Networks, Elsevier, vol. 87, (2015), pp. 44-58.
[31]. G. Kim, Y. Han and S. Kim, "A cooperative-sinkhole detection method for mobile ad hoc networks", AEU-International Journal of Electronics and Communications, Elsevier, vol. 64, Issue5, (2010), pp. 390-397.
[32]. K. S. Arathy and C. N. Sminesh, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET", Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, Procedia Technology, Elsevier, vol. 25, (2016), pp. 264-271.
[33]. N. Khanna, (2016) "Mitigation of Collaborative Blackhole Attack using TRACEROUTE Mechanism with Enhancement in AODV Routing Protocol", IJFGCN, SERSC Publishers, vol. 9, Issue 1, (2016), pp. 157-166.
[34]. A. Dorri, "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET", Wireless Networks, Springer, vol. 23, Issue 6, (2017), pp. 1767-1778.
[35]. T. Poongodi and M. Karthikeyan, "Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Wireless Personal Communication, Springer, Vol. 90, Issue 2, (2016), pp.1039-1050.
[36]. H.-M. Sun, C.-H. Chen and Y.-F. Ku, "A novel acknowledgment-based approach against collude attacks in MANET", Expert Systems with Applications, Elsevier, vol. 39, Issue 9, (2012), pp. 7968-7975.
[37]. J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao and C.-F. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE Systems Journal, vol. 9, Issue 1, (2015), pp. 65-75.
[38]. Nitin Khanna, Monika Sachdeva (2018), "A Comprehensive Review of Mitigation Techniques for Blackhole Attack in AODV Routing Protocol in MANETs", IJAST, Vol. 111, February, 2018.
[39]. Nitin Khanna, Monika Sachdeva (2018), "Critical Review of Techniques for Detection and Mitigation of Co-operative Blackhole Attack in MANET", IJAST, Vol. 110, January, 2018.
[40]. Priyanka Sharma, Nitin Khanna (2017) "FANET: A Review Study", International Journal for Science and Advance Research, Vol. 3, Issue 9, September, 2017, pp. 483-487.
[41]. Nitin Khanna, Priyanka Sharma (2017) "Survey On Delay Tolerant Network And It's Rfc 4838 Architecture", Asian Journal of Mathematics and Computer Research, Vol. 18, Issue 4, June, 2017, pp. 168-176.
[42]. Nitin Khanna, Priyanka Sharma (2016) "Mitigation Balckhole and Grayhole Attack in MANET using Enhanced AODV with TLTB mechanism", IJFGCN, Vol. 9, Issue 8, January, 2016, pp. 129-140.
[43]. Nitin Khanna (2016) "Avoidance and Mitigation of All Packet Drop Attacks in MANET using Enhanced AODV with Cryptography", IJCNIS, Vol. 8, Issue 4, April, 2016, pp. 37-43.