Advances and Applications in Mathematical Sciences
Volume 19, Issue 6, April 2020, Pages 517-532
© 2020 Mili Publications

A NOVEL APPROACH TO DETECT BLACKHOLE ATTACKS IN MANET

SEEMA, RAJDEEP KAUR and RENU BALA

Computer Science and Engineering
College of Engineering
Chandigarh Group of Colleges
Landran, India
E-mail: seema.3844@cgc.edu.in
rajdeep.4420@cgc.edu.in
renu.4405@cgc.edu.in

Abstract

MANET could be a network that's infrastructure-less and therefore the nodes during this network will solely communicate with farther nodes in multi-hop manner. The nodes possess the property of quality and route is created on ad-hoc basis as per requirements. Because of this characteristic nature of MANET, it's susceptible to several routing and security attacks. The foremost hazardous and customary among those attacks is Blackhole attack that could be a reasonably packet drop attack. The variation of Black-hole attack additionally proves to be unsafe once dead intelligently. The variations of Blackhole attack like Grayhole attack and co-operative attack in conjunction with commonplace Blackhole attack becomes a bottleneck within the potency of secure MANET routing. During this paper, a mechanism is planned which will mitigate the result of every kind of Blakchole attack and its variations. For it, a Bogus destination is employed to create a lure for the malicious nodes and use of AODV routing protocol is formed for correct detection of Blackhole attack. This work is compared with printed work EDRI (Extended knowledge Routing Information) and TLTB (Traffic lightweight Trust Based) mechanism against parameters like Packet Delivery quantitative relation, Normalized management Load, dependability of path fashioned and Accuracy of detection of offensive nodes in MATLAB 2017a surroundings.

I. Introduction

MANET stands for Mobile ad-hoc network that contains movable nodes that may move freely in any direction through a random movement model

2010 Mathematics Subject Classification: 90B18.

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

Received 18 November 2019; Accepted 16 December 2019

[38] or a delegated movement model. The nodes in movement will show regular or irregular pattern relying upon the sort of model used for movement. Because of ad-hoc nature the routes area unit fashioned according the requirement in an exceedingly spontaneous manner. Because of these intrinsic proper-ties of Manet, this sort of network is vulnerable to varied security attacks like routing attacks, packet attack, and knowledge spoofing and alternative sorts of security and repair attacks. Manet could be a suburbanized [1] infrastructure-less network that has no central dominant system, therefore it paves the manner for offensive nodes to disrupt the communication and varied mechanisms has been devised for mitigation of various kinds of Manet security and routing attacks. For knowledge routing in Manet different reasonably routing protocols like DSR [9] (Dynamic supply Routing) protocol, AODV [10]. These routing protocol area unit typically classified as re-active formation and maintenance. Re-active routing protocol [8] formulates the trail only it's required and can not notice the trail even supposing it's thus far ne'er required to formulate. Pro-active routing protocol [8] maintains all the routes all the time whether or not it's required or not and therefore causes the overhead of maintenance of ways which will ne'er be required whereas Hybrid routing protocol could be a mixture of each re-active and pro-active schemes of routing within which at native level pro-active mechanism is employed whereas for more nodes re-active mechanism is employed.

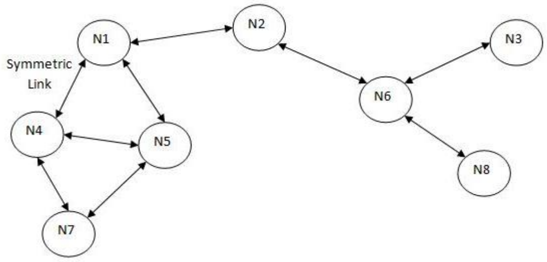


Figure 1. Mobile Ad-hoc Network.

Pro-active routing protocols offer all the routes whether or not those area unit required or not and therefore cause overhead because of the trouble wasted in establishing routes that may ne'er be used. On the opposite hand, re-active routing protocols initiates the route discovery method only the route is needed and during this manner causes tokenize overhead of route maintenance of these routes that may ne'er be required however a delay [41] in route formation is concerned just in case a route that wasn't previously established however required currently. This happens once a supply must communicate to specific destination to that no alternative node has thus far communicated and therefore no path thereto destination has been developed and clearly high quantity of packet overhead are going to be concerned to determine a route thereto particular destination. The selection of underlined routing protocol has result on the mechanism that's utilized for providing security against varied attacks within the Manet and therefore must be showing wisdom chosen at the initial stage.

Packet drop attacks like Blackhole [6, 38], Grayhole [2] and co-operative Blackhole [21-22, 32, 39] area unit the foremost catastrophic attacks in Manet if not detected through the utilization of effective detection mechanism. Blackhole attack could be a reasonably attack within which the offensive node act as a Blackhole by replying with a faux RREP packet in response to a RREQ packet sent earlier by some supply node, that RREP packet can have higher price of destination sequence variety and comparatively low hop-count price to persuade the supply node that it's the shortest and contemporary most path to the actual destination. However really it doesn't have any route thereto destination and therefore is simply acting malicious trying to find chance to hamper communication by dropping any knowledge packets routing through it. Once the supply node sends knowledge packets there to destination.

Through this Blackhole node that's acting as a legitimate intermediate hop, the Blackhole node drops every and each knowledge packet to disrupt any communication between those 2 finish nodes. This can be the foremost basic and ordinarily dead packet drop attack however with nice consequences that may sway be terribly unsafe if no security mechanism [12] is deployed. Several mechanisms area unit researched and devised that may notice Blackhole attack in effective manner however still it's an awfully serious and commonest threat to the effective routing in Manet.

Grayhole attack, on the opposite hand, could be a special reasonably Black-hole attack within which the offensive node drops packets selectively and forwards the remaining and therefore it's terribly tough to notice this kind of attack victimisation mechanism devised for Blackhole attack detection. This packet drop attack is incredibly rigorous because it is incredibly tough to formulate a mechanism that may accurately diversify a malicious attack from AN unwilling collusion because of wireless link transmission that forms the premise of false positive. This attack is but, tough to execute and complicated in its true sense because it is driven by a synthetic Intelligence or AN intelligent adaptative program within the malicious node for continuous choice of packets that's to be born whereas forwarding others that seem as honest node to the opposite honest nodes within the network and doesn't acquire notice if easy packet drop mechanisms area unit utilised.

Lastly, Co-operative Blackhole attack could be a mega style of Blackhole attack within which 2 or a lot of malicious nodes in co-ordination performs the packet dropping action. One node within the co-operation supply and once an information packet is distributed through it; it forwards it to its malicious co-operative node that performs the packet dropping action. Therefore each the nodes perform the packet dropping along attack while not coming back into notice to alternative nodes within the Network.

II. Related Work

In this section, some printed works area unit reviewed that come back from varied authors that has solutions for detective work and mitigating packet drop attacks [11] and supply security to the communicated data from passive attacks. Watchdog [7] and Pathrater [7] area unit the mechanisms that area unit wide used for detective work Blackhole attack. Pathrater [7] mechanism is employed to avoid forming routes that features Blackhole nodes. This mechanism uses a rating methodology between zero and one and Blackhole nodes area unit given -100 rating that's minimum of all. The dependability of path is calculated from the typical of path rating of the nodes concerned within the formation of that path. Thus, if the trail involves a malicious node then its path rating would be terribly low and no such path is taken into account by the node a good variation of normal Watchdog mechanism is formulated by totally different authors for a lot of correct Blackhole detection. Theorem Watchdog [13] and Kalman Watchdog [5] uses filters which will facilitate in circumstantially notice Blackhole and avoid false positives and true negatives. These mechanisms use complicated equation for hard the dependability and trust level of nodes and nodes area unit thought-about malicious as long as they yield a result below threshold when calculation through complicated filter equations. Structure Threshold Secret Sharing [16]. These techniques offer sensible knowledge security however puts high quantity of load on the processor of mobile nodes. These techniques result in high security overhead as they need complicated calculations at each ends that takes heaps of time interval and energy. Collaborative Watchdog [4] is additionally used for exactly detective work Black-hole attack and disseminates this data to alternative nodes within the network. The knowledge regarding their neighbor node and helps in diffusing information regarding malicious nodes. This work from suppositious purpose of read is nice however neglects the foremost vital issue of power consumption is Manet. In [3], cryptography is employed to boost security of the routing protocol that has greatest dependability however the handling of cryptography is incredibly inefficient that ends up in a lot of power dissipation of nodes that is crucial in Manet. Enhanced W-AODV [15] that features varied new fields provides higher security however don't notice co-operative attacks. Trueness Level [14] helps in forming reliable routes in an exceedingly a lot of economical manner and proves to be wonderful in reference to changed AODV routing protocol. Exactness Level [14, 25] provides an easy rule to get a trust hierarchy and co-operation among honest nodes for malicious node detection and dissemination of such data.

CORIDS [24] tries to avoid Blackhole attack and notice once occur on the premise of cluster formation within which clusters per-forms the particular detection and routing method. Increased temporal windowing [26] performs cross-layer collaboration for detection of attacks by seeing the variation between RTS/CTS quantitative relation with the particular packet delivery quantitative relation. A threshold price is used to substantiate the variation as attack. EMLTrust [27] mechanism relies on the educational of the network to adapt to dynamical situations however needs high degree of complicated algorithm. Anomaly primarily based IDS [30] offer a windowed methodology for detective work the Blackhole attack by considering solely the cur-rent behaviour of nodes. Co-operative mechanism [31] makes use of many packets for indication of depression however causes a lot of overhead. TRACEROUTE

[33] mechanism uses the anomaly detection approach for breaking the co-operative at-tack collaboration by victimisation trace and Reverse TRACE packets. Cooperative theorem Watchdog [18] makes uses of Bayesian filter for correct detection of offensive nodes victimisation inference. However, it additionally causes high degree of overheads within the network. LSAM [35] uses AN acknowledgment primarily based approach that uses a sequence variety primarily based approach in conjunction with threshold price for any Blackhole attack or its variations detection. CBDS [37] uses a bait destination for correct detection of Blackhole attack with the assistance of intrinsic property of DSR protocol.

III. AODV Routing Protocol

Ad-hoc On-Demand Distance Vector Routing Protocol [23] could be a reactive routing protocol within which route is created as and once required on demand. AODV uses four management packets; RREQ (Route REQuest), RREP (Route REPly), RERR (Route ERRor) and greeting packets for establishing the routes and exchange data with neighbourhood and alternative nodes within the network regarding the reachability. It uses the idea of the sequence variety and Broadcast-ID which will facilitate in maintaining most contemporary routes and avoiding the ne'er ending flooding of route institution packets. the upkeep of routing table is completed at every node in such how that each one the intermediate nodes to the trail store consecutive hop within the path to a particular destination with a desired high and valid sequence variety. It uses broadcast-ID field in its packet that in conjunction with destination address forms a singular entry for the RREQ packet that facilitate in keep a check on flooding of RREQ message throughout route discovery method. Greeting [23] messages area unit changed at regular interval by all the nodes with its neighbourhood to inform the opposite nodes within the network that area unit in its direct communication vary regarding its reachability. The method of route discovery is explained through following figures:

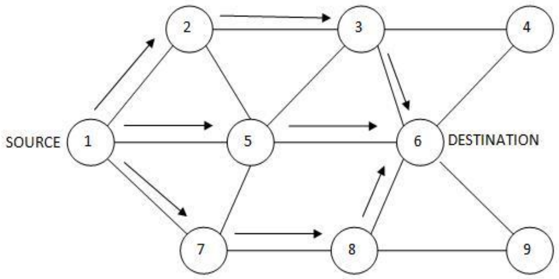


Figure 2. Route Discovery by causing RREQ packet.

In the figure on top of, supply node one broadcasts RREQ packet to seek out a path to destination node half-dozen and on receiving the RREQ packet with destination half-dozen, if any intermediate node has path thereto node then it'll respond with RREP packet, otherwise it re-broadcasts RREQ message by increasing the hop count by one.

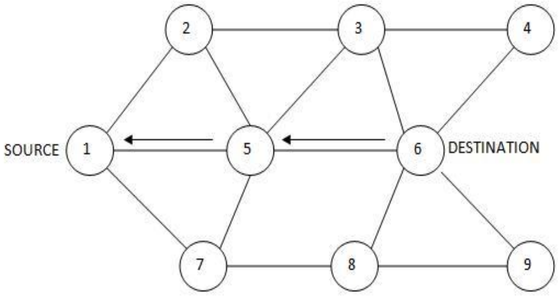
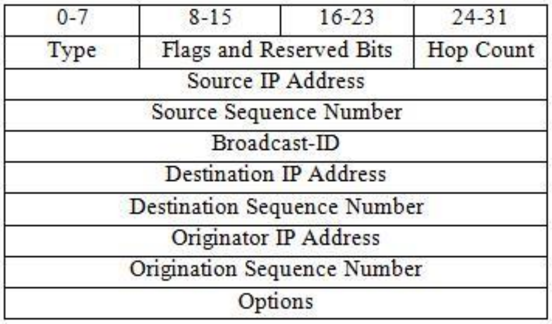


Figure 3. Destination causing RREQ packet.

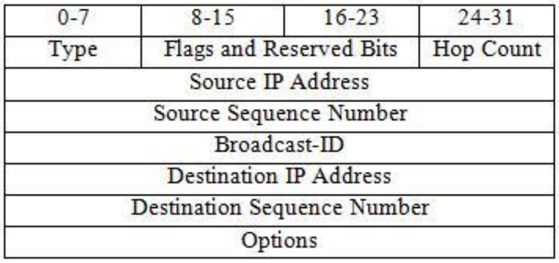
On receiving RREQ packet, node half-dozen finds out that it's for itself and therefore it responds with a unicasted [19, 40] RREP packet with its own destination sequence variety. All the intermediate hops within the path update their routing table and unicasts the RREP packet towards the supply node one.

The header format for RREQ and RREP management 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			

Figure 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			

Figure 5. Format of General RREP packet [43].

IV. Proposed Methodology

In this section a Blackhole attack detection mechanism is presented that uses the standard AODV routing protocol and its management packet to spot the offensive node. Firstly, as we all know that a Blackhole node that's meant to perform packet dropping action can try and attract traffic through it by advertising itself as being having the foremost optimum and shortest route.

In current state of affairs and once the supply sends an information packet to the destination through it, then it drops the packet and disrupts the communication. So, here a theme known as Bogus destination routing is given within which a random honest node tries to seek out path to a phony destination, i.e., a destination node that doesn't exist. Obviously, no alternative honest node has path to the current Bogus node and cannot reply with a path. Solely the Black-hole node can respond with a faux path and once the supply node finds out the RREP packet is received for a Bogus RREQ packet then it marks that as Blackhole.

Here to begin with, the supply node that desires to notice a Blackhole node within the network in its communication vary can initiate the procedure by broadcasting a RREQ packet that involves a Bogus destination that doesn't exists within the net-work. This RREQ packet is not any totally different from an everyday RREQ packet except the very fact that it contains request for the route to a destination that doesn't exists which too is just legendary to the mastermind of this RREQ packet. The broadcast-ID for this packet is hold on for more verification of received RREP packet. All the nodes that area unit non-attacking honest nodes on receiving this Bogus packet can forward it to their several neighbourhood by simply dynamical the hop count field. Solely the active Blackhole node on receiving this RREQ packet can reply with a RREP packet that contains a faux hop count and a high price of destination sequence variety to confirm supply node that it's the shortest and most contemporary path to the required destination node. The Blackhole node that is generating this RREP packet has got to embrace its own information science address and sequence variety in order that supply will determine generator of RREP packet. So, once the RREP packet received by the supply node then it checks the broadcast-ID of the RREP packet initial, if that ID matches with any of the hold on broadcast-ID [43] that's used for Bogus destination then the mastermind of the packet is marked as Blackhole and therefore the data is disseminated within the entire network.

To elucidate the methodology, here a situation is taken into account within which there area unit ten nodes within the network with one Blackhole node as shown within the following figure:-

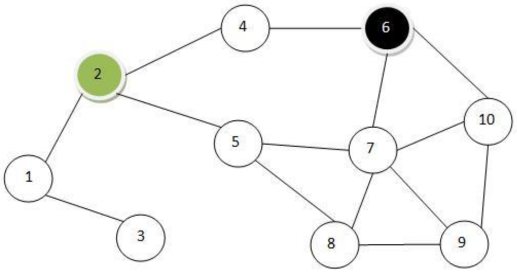


Figure 6. Illustration of Bogus node coping with Blackhole Attack.

In the figure on top of node half-dozen is that the Blackhole node whereas node two is that the node that initiates the detection method by presumptuous a Bogus destination that doesn’t exists and tries to seek out a path thereto destination. It generates a RREQ packet and broadcast it within the network and maintains the broadcast-ID of that RREQ packet within the list. All alternative honest nodes within the net-work like Node one, Node four and node five won’t have route to the current bogus destination so that they re-broadcast it to their neighbourhood. Once ultimately this RREQ packet reaches node half-dozen.

Which could be a Blackhole node, and then it generates a faux RREP packet with some false hop count and send it towards the supply node two with its information science address and sequence variety in respective fields of RREP packet. On receiving the RREP pack-et generated by Blackhole node half-dozen, node two checks the broad-cast-ID of RREP packet and matches it with hold on price within the list. If there’s a match then supply node two understands that it absolutely was for the aim of detection and therefore the destination doesn't exists And if there’s any RREP packet coming back in response thereto then it should be coming back from an offensive Blakchole node. Therefore node two marks node half-dozen as Blackhole and broadcast the detection data to the opposite nodes within the network.

V. Simulation Environment

All the simulations and demanding analysis of outcome is completed in MATLAB 2017a surroundings. The planned work Bogus node has been compared with the printed work Extended knowledge Routing Table [34] (EDRI) and light Trust primarily based (TLTB) [42] mechanism. All the supply nodes within the network send 512 computer memory unit sized knowledge packets excluding the header of packet. The simulation is completed beneath static surroundings within which some parameters area unit fastened and a few parameters of environment area unit varied to get multiple situations. The assumed surroundings and parameters used for simulation of planned work area unit delineated within the table below:

Table 1. Simulation surroundings 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

VI. Result and Discussion

In the experimental simulation, the planned work Bogus destination has been evaluated against 3 parameters; Pack-et Delivery quantitative relation, Accuracy in detection of Blackhole and its variants and Normalized management Load. The results for the planned work for these parameters area unit then compared with the printed work Extended knowledge Routing data (EDRI) [34] mechanism and light Trust primarily based Mechanism (TLTB) [42]. When comparison, the ensuing graphs area unit then mentioned to elucidate the impact of the planned approach in AODV routing protocol usage in vulnerable Manet network. The results area unit calculated by varied each density of offensive Blackhole nodes, node density within the network and Mobilise speed of nodes. The network parameters area unit compared in graphical kind with varied node quality that involves a numeral figure through averaging the values of alternative parameters at totally different node densities and offensive Blackhole densities, i.e., by dynamical variety of nodes within the network in conjunction with dynamical the quantity of Blackhole nodes and keeping node quality constant for that point. The result on the basis of various network parameters area unit shown and argued as follow:

A. Packet Delivery quantitative relation (PDR) v/s Node quality

Packet Delivery quantitative relation is calculated through the quantitative relation of total variety of packets received by desired destination node and therefore the total variety of packets generated at the supply node for that desired destination node. The upper the Packet Delivery quantitative relation within the network any instance, higher are going to be the potency and effectiveness of the network at same instance. It must get on the upper facet continually at any node quality speed and even in presence of any reasonably offensive nodes in any variety to create the mechanism appearance effective in its method and advantageous for the user.

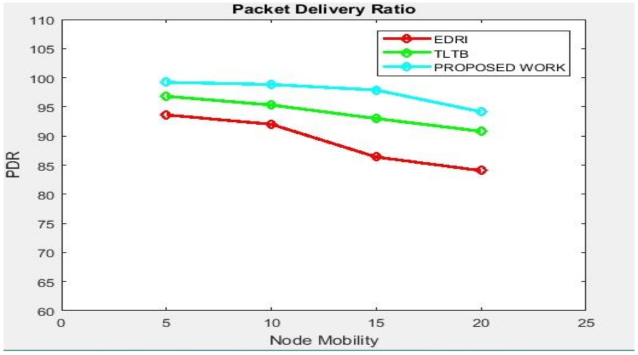


Figure 7. Packet Delivery quantitative relation Comparison between planned and printed works.

In the figure on top of, through comparison of the planned work with EDRI and TLTB mechanism, it's clearly visible that varied the quality speed in conjunction with alternative parameters like node and Blackhole node densities won't have an effect on abundant even at higher degree of quality. The PDR level stays on top of ninety fifth even at the highest twenty m/second quality speed whereas the opposite 2 printed work shows a declined in PDR at high speed this can be because of the very fact that the Blackhole node detection method doesn't rely upon the routing pattern. It entirely supported faux destination to lure the offensive node and therefore doesn't show abundant variation at high speed. The sole decline in PDR is just to the very fact that path area unit broken sooner at high quality speed if the movement pattern isn't elegant.

B. Normalized management Load v/s Node quality

Normalized management Load is calculated because the quantitative relation of total variety of management Packets generated by nodes within the network for route generation and maintenance and therefore the total variety of knowledge Packets received by the required destination nodes and absolutely acknowledged. Normalized management Load ought to be at lower facet. However, it's absolute to increase with high degree of quality speed and if the node density isn't inflated in conjunction with that in larger proportion. This happens due to the very fact that at higher quality the trail got non-continuous comparatively quickly because of calling it quits of links between some neighbor nodes.

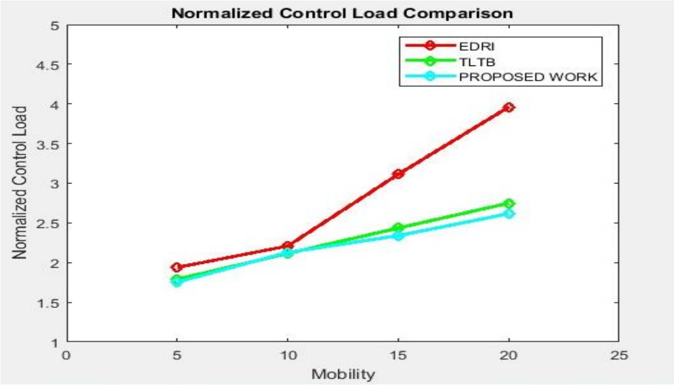


Figure 8. Normalized management Load Comparison.

From the comparison in on top of figure, it's clearly visible that the planned work provides lower normalized management load at comparatively higher degree of quality speed and therefore the quality speed pattern has little or no impact thereon which to solely because of disruption of links between neighbourhood and undue to causing multiple management packets for detection of attack in network whereas for alternative printed work, the impact on control load is because of disruption of route yet as ruinous result of malicious activities of Blackhole nodes that go undetected because of higher quality rates.

Accuracy in Packet Drop Attack Detection v/s Node Mobility

Accuracy in detection of Blackhole attack and its variants is calculated by computing the quantitative relation between total varieties of offensive nodes discovered by the mechanism and therefore the total variety of offensive nodes really exists within the network. Because the accuracy rate is measured in share therefore the quantitative relation result is increased by a hundred to urge the ultimate accuracy rate. The mechanism utilized must be extremely correct to be of appropriate and usable in actual Manet surroundings that are obviously vulnerable to terribly malicious attacks like Blackhole and its variants.

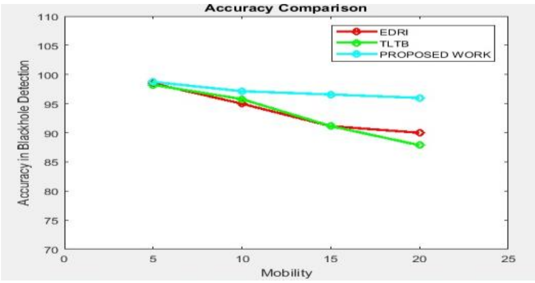


Figure 9. Accuracy in Packet Drop Attack Detection Comparison.

As it clear from the comparison in on top of figure that planned mechanism is extremely correct even at varied quality speed in any situation and shows an awfully steep decrease at higher value of mobile speed. On the opposite hand, remainder of the compared printed work shows larger decrease in accuracy because of false positive and true negatives that has major impact at high quality speed. The planned work is free from false positive and true negative and because it is just dependent upon a Bogus destination and a faux RREP packet reception from offensive node that doesn't rely upon the mobile speed. Therefore the mechanism is extremely correct. The little steep in accuracy at high quality rate is because of the very fact of dropping of pretend RREP or RREQ packet for Bogus destination at high speed of mobility.

VII. Conclusion

Packet drop attacks like Blackhole attack and everyone its variants will sway be terribly unsafe if not handled in their origin state. So, this issue must be managed and sorted out through a detection or mitigation mechanism during akin an exceedingly in a terribly very effective and economical manner. The mechanism planned during this paper helps in distinctive and eliminating every kind of variants of Blackhole attack that too while not hampering the graceful communication and increasing the overhead on the network. The mechanism makes use of bogus destination that doesn't exists and detective node waits for the faux RREP packet from the offensive node and so mark it as malicious and broadcast the knowledge within the entire network. The detection doesn't involve high calculation or additional bur-den on processors or network equipments and has is nearly free from process and network overheads. The accuracy is additionally of upper degree for a similar reason because the mechanism will work well at any quality speed that too with least management overhead.

As future work, it's planned to boost the mechanism to create the dissemination of knowledge free from faux detection report while not increasing the network and process overhead. Additionally thereto a special routing attack, Worm-hole attack [1] may also be thought-about for its mitigation.

References

[1] Punya Peethambaran and J. S. Jayasudha, Survey of Manet Misbehaviour Detection Approaches, International Journal of Network Security & Its Applications 6(3) (2014).

[2] Gaurav, Naresh Sharma and Himanshu Tyagi, An Approach: False Node Detection Algorithm in Cluster Based MANET, International Journal of Advanced Research in Computer Science and Software Engineering 4(2) (2014).

[3] K. Sahadevaiah and Prasad Reddy, P.V.G.D., Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks, Macro Think Institute 3(4), 2011.

[4] Enrique Hernández-Orallo, Manuel D. Serrat, Olmos Juan-Carlos, Cano Carlos, T Calafate and 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 and Pankaj Sharma, An Improved Watchdog Intrusion Detection Systems In Manet, International Journal of Engineering Research & Technology 2(3) March 2013.

[6] Vrutik Shah and Nilesh Modi, An inquisition based Detection and Mitigating Techniques of AODV Protocol in Existence of Packet Drop Attacks, International Journal of Computer Applications 69(7), 2013.

[7] D. Anitha and M. Punithavalli, A Collaborative Selfish Replica with Watchdog and

Pathrater in MANETS, IJCSMC, 2(3), pp. 112 – 119, March 2013.

[8] Carlos de Morais cordeiro and Dharma P. Aggarwal, Mobile Ad-hoc Networking, 2004. Andreas Tonnesen-Mobile Ad-hoc Networks, 2004.

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

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

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

[12] M. D. Serrat-Olmos, E. Hernandez-Orallo, J. Cano, C. T. Calafate and P. Manzoni, Accurate detection of black holes in MANETs using collaborative bayesian watchdogs, Wireless Days(WD), IEEE Conference (2012), 1-6.

[13] R. L. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21(2) (2013), 120-126.

[14] Nitin Khanna and Parminder Singh, Mitigating Blackhole and Security attacks in MANET using Enhanced W-AODV with Trueness Level and Cryptography, IJRECE 3(2) (2015), 146-151.

[15] Lein Harn and Miao Fuyou, Multilevel threshold secret sharing based on the Chinese Remainder Theorem, Information Processing Letters 114, ELSEVIER (2014), 504-509.

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

[17] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang and 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.