International Journal of Future Generation Communication and Networking
Vol. 9, No. 8 (2016), pp. 129-140
http://dx.doi.org/10.14257/ijfgcn.2016.9.8.13

Mitigating Blackhole and Grayhole Attack in MANET using Enhanced AODV with TLTB Mechanism

Nitin Khanna[*,1] and Priyanka Sharma[2]

[1]*Assistant Professor, Department of Computer Science, Lyallpur Khalsa College, Jalandhar*
[2]*Assistant Professor, Department of Computer Science & Engineering, College of Engineering and Management, Kapurthala*
[1]*nitinkhanna300@gmail.com*, [2]*Priyasoni289@gmail.com*

Abstract

MANET is multi-hop network which is a decentralized and infrastructure-less network that includes collection of mobile nodes that are self configurable and co-operates with each other for transmission of data. It has dynamic nature in terms of topology. Due to this dynamic nature of topology and no fixed infrastructure in MANET, these nodes have to be dependent on each other for transmission of data and thus are prone to packet drop attacks like Blackhole, grayhole attack. These attacks hinder the smooth transmission of data between nodes and hampers effective communication. In this paper, a new mechanism Traffic Light Trust Based (TLTB) is proposed to detect both Blackhole attacks and Grayhole attacks. This mechanism works after modification in the standard AODV routing protocol and Watchdog mechanism. This mechanism uses color scheme to define trust level of a node or any path. Just like traffic light it includes three colors to depict the level of trust. AODV routing protocol packets are modified to include new fields for application of proposed trust mechanism. These Solutions are compared with Light-weight Trust Based (LTB) and EDRI mechanism for Normalized Control load, Packet Delivery Ratio, accuracy in Blackhole and Grayhole detection and reliability of paths.

Keywords*: Blackhole Attack, Enhanced AODV, Grayhole Attack, MANET, TLTB (Traffic Light Trust Based) Mechanism*

1. Introduction

MANET is a mobile Ad-hoc Network which is a decentralized network that has no infrastructure and the mobile nature comes from the fact that nodes in the MANET can move freely in the network according to a regular or irregular pattern. The ad-hoc nature comes from the fact that the routes are formed as and when needed and there are no fixed routes between two end nodes. MANET is a hop by hop delivery network in which the nodes act as router for delivery of data from source node to destination.

Various routing protocols are used to formulate a path between source and destination. Various routing protocols include DSR [8], AODV [10], OLSR [9], etc. All these protocols are divided into pro-active, re-active or hybrid category [22] depending upon the instance at which the route is formed. Out of all these routing protocols AODV proves to be the fascination of researchers which is a re-active routing protocol that determines the route only when it is needed. It includes three packets for route discovery that are RREQ [10], RREP [10] and RERR [10]. RREQ packet is used to send a request to found an optimized route by source or any intermediate node. RREP packet is sent back to the source by destination or any intermediate node having a route to the destination. While RERR packet is used to report any error in route formulation.

Due to the ad-hoc nature of MANET, it is very prone to packet drop attacks that are injected at the time of route discovery. The main packet drop attacks include Blackhole

ISSN: 2233-7857 IJFGCN

[1] attack and grayhole [1] attack. Blackhole attack is an attack in which the malicious node fakes a route to a particular destination from itself and when the source node sends a packet to the destination through it, it maliciously drops all the packets. To counter this Blackhole attack a commonly used mechanism called Watchdog is used that maintains a counter at each node for every other node in the network. In this mechanism, when a node in the network sends a packet to next node it increments the counter by 1 for that particular node. When the next node forwards that packet further in the path, that counter is decremented. If the next node does not forward the packet, the counter remains unchanged for that particular node and when the counter reaches to a particular threshold then that next node is marked as blackhole by the node and it notifies the source about it.

Grayhole attack, on the other hand, is a special case of Blackhole attack in which the malicious node does not drop all the packets routed through it but drops only some selective packets so that it can escape from the Watchdog [7] mechanism. It is more brutal form of packet drop attack as it can go undetected using Watchdog mechanism if planned well.

To counter Blackhole and Grayhole attacks, we proposed a scheme called TLTB (Traffic Light Trust Based) mechanism that uses a color scheme for identifying the reputation of the node and the path formed between two end nodes. This scheme requires modification of routing packets used in the routing protocol AODV. AODV is modified to include additional fields to form the basis for working of TLTB mechanism. In the remaining of the research paper, we will first of all present related work in this field. After that we provide the methodology of our work that includes modification of AODV routing protocol followed by TLTB mechanism and its working. After that we will present the simulation environment followed by result and discussion that will reason about the implementation and working of our mechanism.

2. Related Work

In this section, we discuss some published works coming from various authors that provides solutions for detecting and mitigating various packet drop attacks [11] like Blackhole and Grayhole attacks. Watchdog [7] and Pathrater [7] are the mechanisms that are most widely and commonly used for detecting and mitigating Blackhole attacks in MANET. Watchdog is used to detect Blackhole nodes by using a counter that is maintained at each node for every other corresponding node in the MANET. This counter is incremented by node only if it does not overhear the forwarding of packet by next hop which it has earlier forwarded to it to pass towards a particular destination. If the counter reaches a predefined threshold value, the next hop in the path, is marked as Blackhole and source node is notified about the detection and marking of Blackhole node. But standard Watchdog is not much accurate due to false positives and true negatives. Pathrater [7] mechanism is used to avoid the formation of routes that are not safe from packet drop attacking nodes that means the paths that includes Blackhole or Grayhole nodes. This mechanism uses a rating method and every node in the network maintains a rating for every other node in the network. The rating lies between 0 and 1 for an undetected malicious node or for a fair node. For detected Blackhole nodes it becomes -100 rating that is the minimum among all. The reliability of path is calculated from the average of rating associated with 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 would be considered by the source node for communication. A wide variation of standard Watchdog mechanism is researched and formed by different authors for more accurate Blackhole detection. Bayesian Watchdog [13] and Kalman Watchdog [5] use filters that will help in minutely detecting the Blackhole nodes and avoid false positives and true negatives. These mechanisms use complex equation for calculating the reliability and reputation of nodes and nodes are considered malicious only if their reputation or trust

value lies below the pre-defined threshold value. But these variations in the standard mechanisms lead to high network overhead as a lot of data is communicated between all the nodes in the MANET for accurate detection. Collaborative Watchdog [4] is also used for precisely detecting Blackhole attack and shares this information to other nodes in the network. This mechanism is based on the co-operation of various nodes in the network that involved in sharing of the information about their neighbouring node and helps in disseminating information about malicious nature of node, if any. 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 after the detection of Blckhole attack. 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 to formulate a new path to that particular destination. 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 a malicious node. It uses further request and further reply [18] message to acquire gray nature of nodes. But it will create lots of network overhead on the storage and processing of tables for each and every node in the network and creates network overload 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 [15] helps in forming reliable routes in a more efficient way and proves to be excellent in connection with modified AODV routing protocol. Trueness Level [15] provides a simple algorithm to generate a trust hierarchy and co-operation among fair nodes for malicious node detection and dissemination of such information. TRACEROUTE [21] mechanism is also very important in the field of MANET as it provides accurate mitigation of co-operative Blackhole attack by using trace packets to break the co-operation among malicious nodes. Enhanced AODV [10] protocol provides addition of new fields that along with the TRUENESS LEVEL [15, 20-21] algorithm provides avoidance from various form of packet drop attacks. Light-weight Trust Based (LTB) mechanism [19] involves light-weight IDS scheme that is flexible enough to use only local information and also some co-operation among neighbouring nodes. This work when use co-operation of neighbourhood leads to high network overhead. Enhanced AODV [20] uses Inceptor field and DR Field for mitigation and detection of both individual and co-operative packet drop attacks. EDRI table [23] used in detection and mitigation of Grayhole attack as it keep track of gray nature of malicious node. It uses further request and further reply [23] message to get information about gray nature of nodes. But it will create huge load on the storage capacity and processing power of nodes and creates network overhead as well for acquiring gray nature of malicious nodes.

3. Methodology

The methodology of our proposed work is divided in two parts. The first part deals with the specification of TLTB mechanism and the remaining part deals with how AODV routing protocol needs to be modified for effective detection of packet drop attacks. The first part, TLTB mechanism includes the basic concept of it and the algorithm for its implementation is discussed in detail. In the second part, the modification of AODV routing protocol in terms of how the structure of its packets is modified.

3.1. TLTB Mechanism

3.1.1. Trust level assignment at node level: This mechanism stands for Traffic Light Trust Based mechanism. It uses a color scheme that defines the trust level or reputation of a particular node as well as trust level of a particular path includes various intermediate nodes. It uses three basic colors involved in the traffic light that are Red, Yellow and Green. These colors are assigned by all the nodes to every other nodes depending upon their performance in forwarding the data packets. In this mechanism, Green color node represents highest trust level while red represents low trust level. Yellow color represents neutral or average level of trust.

Table 1. TLTB Color Scheme for Node Trust Level

COLOR	TRUST LEVEL
Green	Highest
Yellow	↓
Red	Lowest

When the network is initiated, no communication has been take place and no node in the network knows about other nodes in the network. At that point of time the node assigns the color Yellow which is neutral trust level color to every other node in the network it can sense and color Green to itself.

After a period of communication is over, the colors associated with nodes with respect to other nodes are updated according to the performance in transmission in data packet and current color of the nodes. This thing may lead to the promotion of a yellow node to the green node with respect to a particular node or may lead to the demotion to red node. Standard Watchdog mechanism provides black color to the malicious nodes that are detected by a node.

3.1.2. Trust Level Assignment at Path Level: Previously we discussed how the color scheme depicts trust of individual nodes. Now we present how the trust level of path is determined by color scheme. The trust level of path would always depend upon the trust level of nodes involved as intermediate nodes in the path. It involves 6 trust level represented by 3 basic colors of traffic light plus a Black color, in total to represent trust level of the path. Black color is used to depict the path that involves detected malicious nodes that caught performing packet drop attacks either Blackhole attack or Grayhole attack. This scheme is presented in following table as shown:-

Table 2. TLTB Color Scheme for Path Reputation

COLOR SCHEME	TRUST LEVEL
Green	Highest
Potential Green	
Yellow	↓
Potential Yellow	
Red	
Black	Lowest

The path calculated is given a color depending upon the number of Red, Green and Yellow intermediate nodes in that path. Depending upon the number of Red, Green and Yellow intermediate nodes three factors G_f, Y_f and R_f are calculated. Depending upon the

sum of these factors, the path is given a color to define its trust value. The three factors are calculated using following equations:-

$$Gf = \mu_g * G_n \quad (1)$$
$$Y_f = \mu_y * Y_n \quad (2)$$
$$R_f = \mu_r * R_n \quad (3)$$

Here μ_g μ_y and μ_r represents the constants of proportionality that defines the weight of Green, Yellow and Red node respectively in the path to define trust level of path. Whereas G_n, Y_n and R_n define the number of Green, Yellow and red respectively in the path from source node to the destination. The number of Green, Yellow and red nodes to a particular destination from source on a particular path can be easily find out through RREP packets G-Field, Y-Field and R-Field respectively. The value of constants in equation (1), (2) and (3) are given as follow:-

$$\mu_g = 0.25 \quad (4)$$
$$\mu_y = 0.05 \quad (5)$$
$$\mu_r = -0.5 \quad (6)$$

3.1.3. Algorithm for TLTB Mechanism

```
Declare TLTB[][],sent[][],forwarded[][]
1)      /* Initialization of color for nodes w.r.t. each other */
FOR i =1 to n Repeat
        FOR j = 1 to n Repeat
                IF i = j
                        Set TLTB[i][j] = Green;
                ELSE
                        Set TLTB[i][j]=Yellow;
                END IF
        END FOR
END FOR
2)      /* Updating TLTB Array */
FOR i =1 to n Repeat
        FOR j = 1 to n Repeat
                Declare Delivery_Ratio
                Set Delivery_Ratio = forwarded[i][j]/sent[i][j]*100
                IF TLTB = Green
                        IF Delivery_Ratio < 95 and Delivery_Ratio >= 85
                                Set TLTB[i][j] = Yellow
        ELSE IF Delivery_Ratio < 85 and Delivery_Ratio >=75
                                Set TLTB[i][j] = Red
                        ELSE IF Delivery_Ratio < 75
                                Set TLTB[i][j] = Black
                        END IF
                IF TLTB = Yellow
        IF Delivery_Ratio >= 95
                                Set TLTB[i][j] = Green
        ELSE IF Delivery_Ratio < 85 and Delivery_Ratio >=75
                                Set TLTB[i][j] = Red
                        ELSE IF Delivery_Ratio < 75
                                Set TLTB[i][j] = Black
                        END IF
                IF TLTB = Red
                        IF Delivery_Ratio = 100
                                Set TLTB[i][j] = Green
```

```
        ELSE IF Delivery_Ratio < 100 and Delivery_Ratio > 85
                        Set TLTB[i][j] = Yellow
                ELSE IF Delivery_Ratio < 75
                        Set TLTB[i][j] = Black
                END IF
            END IF
        END FOR
END FOR
3)      /* Calculation of Path Trust with TLTB of intermediate nodes */
DECLARE RFactor, YFactor, Gfactor, TrustFactor, TLTB_Path
// RFactor, YFactor and GFactor are calculated using equation (1), (2) and (3) respectively
Set TrustFactor = Rfactor + Yfactor + Gfactor
IF TrustFactor > 1
        Set TLTB_Path = Green
ELSE IF TrustFactor <= 1 and TrustFactor > 0.5
        Set TLTB_Path = Potential Green
ELSE IF TrustFactor <= 0.5 and TrustFactor > .2
        Set TLTB_Path = Yellow
ELSE IF TrustFactor <= 0.2 and TrustFactor > 0
        Set TLTB_Path = Potential Yellow
ELSE IF TrustFactor <= 0 and TrustFactor > -0.25
        Set TLTB_Path = Red
ELSE
        Set TLTB_Path = Black
END IF
```

3.2. Enhancement in AODV Routing Protocol

AODV Routing protocol is a re-active routing protocol that uses RREQ and RREP packets for formation of path in MANET. This protocol is modified to enhance its capabilities by introducing new fields in it. We introduced three new fields each of 8 bits in length. These three fields describe the number of Green, Yellow and Red intermediate nodes in the path. In the RREQ packet includes three new fields that are GIN field, YIN field and RIN field. When source node generates the RREQ packet it forwards the packet to all its neighbouring nodes by incrementing either GIN or YIN or RIN field depending upon TLTB status of the next hop. The intermediate nodes forward the RREQ packet to their neighbours using the same approach. The structure of RREQ and RREP packet in enhanced AODV is presented as follow:-

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			
Padding	RIN Field	YIN Field	GIN Field

Figure 1. Enhanced AODV RREQ Packet

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			
Inceptor IP Address			
Inceptor Sequence Number			
Padding	RIN Field	YIN Field	GIN Field

Figure 2. Enhanced AODV RREP Packet

When the RREQ reaches the intended destination or any intermediate node that has route for that intended destination, The RREP packet is generated by that node making correct updation in the GIN, YIN and RIN fields using their routing tables. As the RREP packet moves toward source node, all the intermediate nodes update their routing table accordingly. No update in RREP is performed by any of the intermediate node. The route table of all the nodes contains three additional fields to keep record for number of Green, Yellow and Red nodes in the path for each route entry. At the source node after the reception of RREP packet, processing is done to rate that path depending upon the value of RIN, GIN and YIN fields that describes number of Red, Green and Yellow intermediate nodes in that particular path. Inceptor Field [20] in RREP packet is used for finding out the intermediate that generates the RREP packet so that source can identify the originator of RREP packet.

4. Simulation Environment

The simulation and analysis of the proposed work is done in MATLAB 2013a. The proposed work has been compared with the published work Light-Weight Trust Based routing protocol (LTB) [19] on the basis of various network evaluation parameters. All the source nodes send data packets of size 512 bytes that exclude the content of header of packet. Each packet includes encrypted data through secret key cryptography. The simulation is done in static environment. The assumed environment and parameters used for simulation of proposed work are described in the table below:-

Table 3. Simulation Environment Parameters and their Values

PARAMETER	VALUE
NUMBER OF NODES	15, 30, 45, 60
SPEED OF NODES (M/SEC)	5, 10, 15, 20
ANTENNA TYPE	OMNI-DIRECTIONAL
% OF BLACK HOLES	10%
% OF GRAY HOLES	10%
AREA	2000 m X 2000 m
NEIGHBOURHOOD TIME	1S
PAUSE TIME	10S
NO. OF SCENARIOS	18
WIRELESS INTERFACE	802.11
ROUTING PROTOCOL	ENHANCED AODV
TRANSMISSION RANGE	250m
ENVIRONMENT TYPE	STATIC
TRAFFIC MODEL	CBR

TRANSPORT PROTOCOL	TCP
MOBILITY MODEL	RANDOM WAY POINT
TLTB UPDATE TIME	5s

Various simulation scenarios are obtained by varying the node speed of mobile nodes and node density that is defined by number of nodes in the network and focus on detection of particular type of packet drop attack.

5. Result and Discussion

During the simulation experiment conducted, the proposed work has been evaluated against four parameters, that are Packet Delivery Ratio, Normalized Control Load, Accuracy in detection of Blackhole and Grayhole attacks and Reliability of path formed and is compared with the published work Light-Weight Trust Based routing protocol (LTB) [19] and EDRI [23] mechanism. After comparison, the results are discussed to enlighten the overall impact of our proposed mechanism in the form of enhancement in AODV routing protocol and introduction of TLTB mechanism. The results are generated by varying both node density and node mobility in the network. The network parameters are compared in graphs with node mobility that is calculated by performing average operation on the values of parameters obtained at various node densities, i.e., by changing number of nodes in the network and keeping node mobility constant at that instant of time. The result on the basis of different network parameters are shown and discussed as follow: -

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

Packet Delivery Ratio is defined as a ratio of total number of packets received by designated intended destination and the total number of packets generated by the source node for that designated intended destination. Higher the Packet Delivery Ratio, higher the effectiveness of network that higher the throughput of the network. It needs to be more than 0.8 at any node mobility speed and even in presence of malicious nodes for network to work in the favor of user to accomplish what is intended from the network.

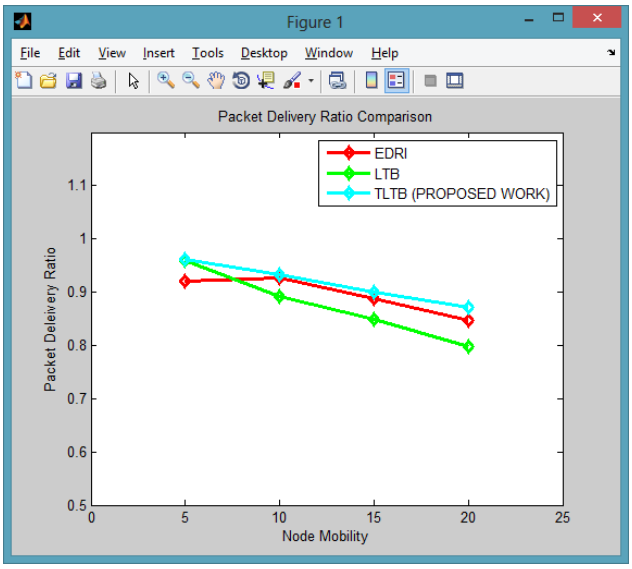

Figure 3. Packet Delivery Ratio Comparison

In the previous figure, through comparison we can easily see that with varying Mobilize speed of nodes, the Packet Delivery Ratio does not show drastic drop even at

higher mobility speed of 20 m/sec. That means, it remains stable over the varying mobility and is consistently touching 90% mark and over, which is better than the comparative work of both LTB [19] and EDRI [23] that shows high drop in PDR as compared to the proposed mechanism. The packet delivery ratio is on higher side in our proposed work as it provides mitigation against Blackhole and Grayhole attacks and form reliable paths due to TLTB mechanism that leads to better and accurate delivery of packets to its designated intended destination.

5.2. Normalized Control Load v/s Node Mobility

Normalized Control Load is defined as the ratio of total number of Control Packets generated by all the nodes in the network to the total number of Data Packets that are received and acknowledged positively by the designated intended destination nodes. Normalized Control Load needs to be in control and minimum even under high mobility and high node density. This network parameter increases with increase in mobility due to frequent breakage of paths between nodes due to unreachability and frequent change of neighbourhood of nodes.

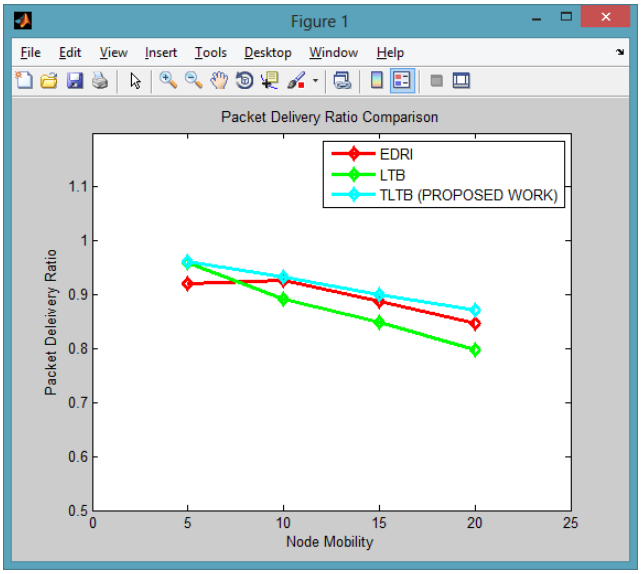

Figure 4. Normalized Control Load Comparison

From the above comparison, it is clear that proposed TLTB mechanism leads to lower control load on network as compared to both EDRI [23] and LTB mechanism [19] and it shows steep increase even at higher level of node mobility. At lower node mobility, the control load is little on the higher side. This is due to fixed cryptographic overhead that can be bear from the security point of view. But as the mobility speed increases to a speed that lies in the range of practical speed used in the MANET, the proposed work performs well and creates only a limited amount of control load even after the inclusion of the cryptographic overheads.

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

Accuracy in detection of packet drop attack is calculated as the ratio total number of packet drop attacks detected by the mechanism to the total number of packet drop attacks actually occurred in the network. It is calculated in percentage so to make that possible the result is multiplied with 100.

The mechanism needs to be highly accurate to be of good use in practical scenarios that are very hazardous to extremely cumbersome attacks like Blackhole and Grayhole attacks.

The accuracy of our proposed work is compared to the published work for detection and mitigation of Blackhole and Grayhole attacks in the network.

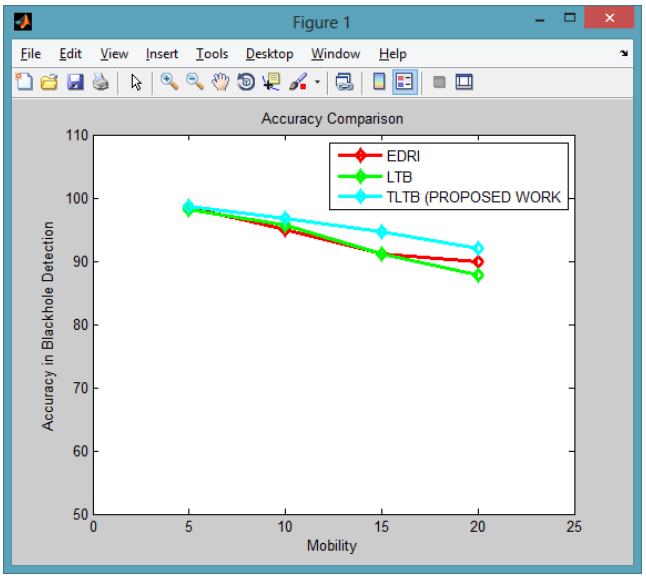

Figure 5. Accuracy in Packet Drop Attack Detection Comparison

From the above comparison, it is clear that our proposed mechanism shows higher level of accuracy in detection of Blackhole and Grayhole attacks even at high mobility among nodes and it shows a minimal decrease even at higher mobility speed of node. The Traffic Light Based Trust mechanism helps in rating the paths accurately so that only reliable paths are formed that contains fair node as intermediate hops. This approach lowers or higher the reputation on trust scale using a color scheme to judge the fairness of node at regular intervals and to keep information of network situation. Inceptor field in RREP packet helps in identifying the source of collaborative Blackhole attack and thus mitigate it indeed. So, these entire enhancement, works in tandem to mitigate and detect various packet drop attacks.

5.4. Reliability of formed Path v/s Node Mobility

Reliability of path formed in the network is measured as security of the path and its freedom from various packet drop attacks, malicious nodes and potential misbehaving nodes. It defines how reliable the path is in long run for transmission of data packets so that no packet dropping attack takes place in that path. Reliability is calculated as the ratio of total number of reliable and attack free path formed to the total number of actual path formed during the entire setup simulative experiment. It is calculated in percentage so for that the result of ratio is multiplied by 100.

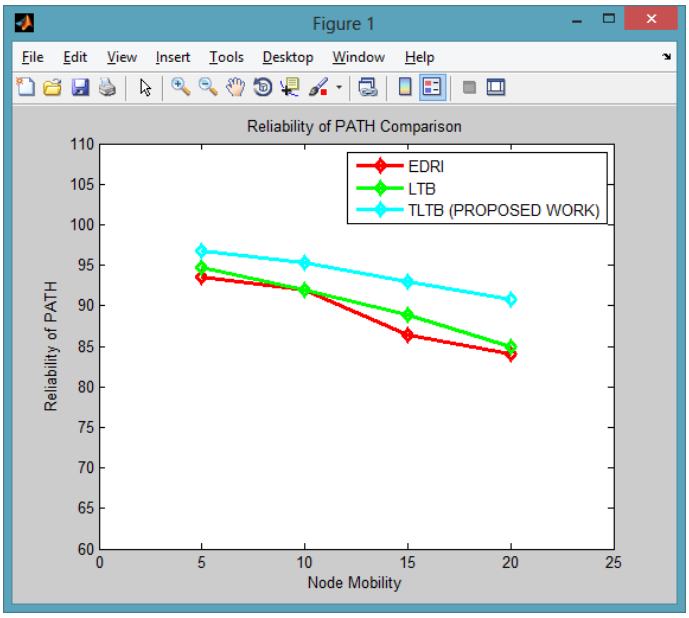

Figure 6. Reliability of Path Comparison

Path reliability decreases with the increase in node mobility again due to breakage of formed path due to unreachability and a little more aggressive chance for malicious node to enter in the network for attack. Still however, the proposed mechanism continuous to form reliable path and shows almost constant lowering even at high mobility speed.

6. Conclusions and Future Work

Blackhole and Grayhole attacks are very sensitive issues in MANET and it needs to be handled with greater efficiency and effectiveness. The proposed mechanism, enhancement in AODV routing protocol using TLTB mechanism helps in identifying, avoiding, mitigating and eliminating all Blackholes and Grayhole attacks that too with greater accuracy and limited network overhead on the network. It increases the Packet Delivery Ratio that is apparent due to the fact that lesser number of undetected attacks and avoidance of packet drop attacks lead to more reliable formation of path that increases PDR. In addition to this, use of cryptography provides security to the data and that too at limited cryptographic overhead. So it can be said that this proposed mechanism provides better security with more reliable paths and better delivery of data packets without putting much load on the network.

As future work, we propose enhancement in mechanism to involve co-operation between nodes at local neighbourhood level for quick detection of attacking nodes and dissemination of information earlier. In addition to that enhancement is proposed to detect a very active form of attack Wormhole Attack [1] that is also a type of co-operative attack leads to disruption of routing process.

References

[1] P. Peethambaran and J. S. Jayasudha, “Survey of manet misbehaviour detection approaches”, International Journal of Network Security & Its Applications, vol. 6, no. 3, **(2014)**.
[2] N. S. Gaurav and H. 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, **(2014)**.
[3] K. Sahadevaiah, P.V.G.D. Prasad Reddy, “Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks”, MacroThink Institute, vol. 3, no. 4, **(2011)**.

[4] E. H. Orallo, M. D. Serrat, O. J. Carlos, C. Carlos, T. Calafate and P. Manzoni, "A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs", Springer , **(2013)**.
[5] T. Sharma, M. Tiwari, P. K. Sharma, M. Swaroop and P. Sharma, "An Improved Watchdog Intrusion Detection Systems In Manet", International Journal of Engineering Research & Technology, vol. 2, no. 3, **(2013)**.
[6] V. Shah and N. 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, **(2013)**.
[7] D. Anitha and M. Punithavalli, "A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS", IJCSMC, vol. 2, no. 3, **(2013)**, pp. 112 – 119.
[8] C. de Morais cordeiro and D. P. Aggarwal, "Mobile Ad-hoc Networking", **(2004)**.
[9] Andreas Tonnesen, "Mobile Ad-hoc Networks", **(2004)**.
[10] C. E. Perkins and E. M. Royer, "Ad hoc On Demand Distance Vector Routing", **(1999)**.
[11] R. H. Khokhar and A. N. S. Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", **(2008)**.
[12] B. A. Forouzan, "Data Communications and Networking", 4th Edition, Tata McGraw Hill Companies, **(2004)**.
[13] M. D. S. Olmos, E. H. 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)**, pp. 1-6.
[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, **(2013)**, pp. 120–126.
[15] N. Khanna and P. Singh, "Mitigating Blackhole and Security attacks in MANET using Enhanced W-AODV with Trueness Level and Cryptography", IJRECE, vol. 3, no. 2, **(2015)**, pp. 146-151.
[16] L. H. M. Fuyou, "Multilevel threshold secret sharing based on the Chinese Remainder Theorem", Information Processing Letters 114, ELSEVIER, **(2014)**, pp. 504–509.
[17] T. Varshney, T. Sharmaa and P. J. Sharma, "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network", IEEE International Conference on Communication Systems and Network Technologies, **(2014)**, pp. 217-221.
[18] G. S. Bindra, A. Kapoor, A. Narang and A. Agrawal, "Detection and Removal of Co-operative Blackhole and Grayhole attacks in MANET", International Conference on System Engineering and Technology, Bandung, Indonesia, September, **(2012)**.
[19] N. Marchang and R. Dutta, "Light-weight trust-based routing protocol for mobile ad hoc networks", IET Information Security, vol. 6, iss. 2, **(2012)**, pp. 77-83.
[20] N. Khanna, "Avoidance and Mitigation of All Packet Drop Attacks in MANET using Enhanced AODV with Cryptography", IJCNIS, vol. 8, iss. 4, **(2016)**, pp. 37-43.
[21] N. Khanna, "Mitigation of Collaborative Blackhole attack using TRACEROUTE Mechanism with Enhancement in AODV Routing Protocol", IJFGCN, vol. 9, iss. 1, **(2016)**, pp. 157-166.
[22] S. Singh and P. Sharma "Mobile Ad Hoc Network", IJETAE, vol. 4, iss. 3, **(2014)**, pp. 473-476.
[23] G. S. Bindra, A. Kapoor, A. Narang and A. Agrawal, "Detection and Removal of Co-operative Blackhole and Grayhole attacks in MANET", International Conference on System Engineering and Technology, Bandung, Indonesia, September, **(2012)**.

