Consensus Routing And Environmental Discrete Trust Based Secure AODV in MANETs

Radha Raman Chandan and P.K.Mishra

Department of Computer Science & DST-CIMS,
Institute of Science, Banaras Hindu University, Varanasi,
rrchandan@bhu.ac.in, mishra@bhu.ac.in

Abstract. The Mobile Adhoc Network (MANET) is a wireless network model for infrastructure-less communication, and it provides numerous applications in different areas. The MANET is vulnerable to a Black-hole attack, and it affects routing functionality by dropping all the incoming packets purposefully. The Black-hole attackers pretend that it always has the best path to the destination node to mislead the source nodes. Trust is the critical factor for detecting and isolating the Black-hole attackers from the network. However, the harsh channel conditions make it difficult to differentiate the Black-hole routing activities and accurate trust measurement. Hence, incorporating the consensus-based trust evidence collection from the neighbouring nodes improves the accuracy of trust. For improving the accuracy of trust, this work suggests Consensus Routing and Environmental DIscrete Trust (CREDIT) Based Secure AODV. The CREDIT incorporates Discrete and Consensus trust information. The Discrete parameters represent the specific characteristics of the Black-hole attacks, such as routing behaviour, hop count deviation, and sequence number deviation. The direct trust accurately differentiates the Black-hole attackers using Discrete parameters, only when the nodes perform sufficient communication between the nodes. To solve such issues, the CREDIT includes the Consensus-based trust information. However, secure routing against the Black-hole attack is challenging due to incomplete preferences. The in-degree centrality and Importance degree measurement on the collected consensus-based trust from decision-makers solve the incomplete preference issue as well as improves the accuracy of trust. The performance of the proposed scheme is evaluated using Network Simulator-2 (NS2). From the simulation results, it is proved that the detection accuracy and throughput of the proposed CREDIT are substantially high and the proposed CREDIT scheme outperforms the existing work.

Keywords: MANETs, Black-hole attack, Security, Discrete trust, Consensus Trust, and Contextual information.

1 Introduction

As the Mobile Adhoc Network (MANET) becomes a critical enabling technology, there is an emerging trend in wireless communication security [1]. The characteristics of unguided medium tend the MANET to be more susceptible to various attacks. Among them, the black hole is the most destructive threat to wireless communication. The black hole attackers modify the functionalities of network layer protocol and advertise themselves as the shortest path to the intended node in MANETs [2, 3]. The primary purpose of black-hole attackers is to proclaim as the nearest route to the intended receiver and to drop all the received data packets. Mostly, the Adhoc On-demand Distance Vector (AODV) routing is a widely used network layer protocol in MANETs[4–7]. The source node starts to broadcast the Route REQuest (RREQ) packet if there is no entry for the current path in the routing table for the intended receiver node. On receiving the RREQ packet, the good intermediate routers ensure either if it is the intended receiver or it has a valid route to the receiver node or not. If a correct path has entered in the routing

DOI: 10.5121/ijcnc.2020.12301

table, a node sends back a genuine Route REPly (RREP) packet otherwise; it continues the RREQ broadcasting. The Black-hole attackers utilize the weakness of the underlying network layer protocol and gives false routing information to launch the black hole attack. The black hole attack deteriorates the routing performance since the routing protocols have generally designed with the assumption of cooperation among the nodes [9–12, 38].

In conventional, there are several trust-based security schemes against the Black-hole attacks in MANETs [13]. The primary process of these techniques is to observe the routing behaviour of MANET nodes in past communications. The trust of a node represents the faith in the routing behaviour of a node. Most of the trust-based security solutions maintain a counter for each neighbouring node and count the packet transmission failures. The transmission failure count of a node increases, only when a neighbour node refuses the data forwarding through a discovered path. By continuously monitoring the neighbourhood activities, the trust management schemes maintain and update the trust value of nodes in MANETs[8]. It is a straightforward scheme to identify the black-hole attack. However, the trust measurement between the nodes does not always represent the actual relationship. Some of the trust-based mechanisms collect the trust values directly and indirectly[33]. The collection of indirect trust information frequently from neighbouring nodes using its direct communication increases the computational complexity and uncertainty to the trust measurement process. Mostly, the trust measurement schemes assume that all the collected trust evidence from the neighbouring nodes are always trustworthy. However, in many cases, it is not reliable. In order to ensure an efficient, secure routing protocol in MANETs without degrading the routing performance, the proposed scheme presents the context-aware routing protocol[40, 43, 44, 41, 42]. This work is organized into the following sections: Section 2 deals with the related works. Section 3 explains in detail about the overview of the Proposed Methodology. Section 4 deals with the experimental evaluation of the proposed algorithm. While Section 5 provides the conclusion and future work for the proposed scheme.

2 Related Works

The Black-hole attack is a packet dropping attack, and such an attack severely deteriorates the routing performance in MANETs. Several defence mechanisms have been proposed to identify and isolate the black-hole attacks in the network.

The Mitigating Black Hole effects through Detection and Prevention (MBDP-AODV) is suggested in [14]. Like [15], it exploits the dynamic threshold value for the destination sequence number. The source node applies mean and standard deviation estimation for multiple RREP packets. In the malicious environment, it is used as the threshold for the destination sequence number. If a source node receives the RREP more than that of the threshold, it is noted as suspected RREP. The source node forwards the suspect packets towards the suspected node. When the intermediate nodes receive the suspect packet, and the hop count is equal to one, then the next-hop node is identified as Black-hole attackers. The major drawback of this protocol is that it cannot mitigate the impact of Black-hole attackers when they act as smart in the network.

To avoid the effects of Black-hole attacks in MANETs, the AODV is enhanced using watchdog nodes in [16]. Using the number of sent and forwarded packets, the trust of each neighbouring node is estimated by the watchdogs. They are responsible for sharing the reputation value of all other nodes in the network. It improves the routing performance under a malicious environment. However, it is inadequate for detecting smart attackers in large scale networks.

To identify the smart Black-hole attackers, the Timer Based Baited Technique (TBBT) and Detecting Black-hole attacks on MANET by using Harmony Search Algorithm (DBHSA) are suggested in [17] and [18] respectively. Each node performs the Baiting phase with random time before sending the data packets to the destination [17]. Within a random time, the source node initiates the bait RREQ into the network. If there is any black-hole node, it replies with the fake RREP packet to the source node. Using such a fake RREP packet, the security scheme identifies the attacker node. By executing the phase of the non-neighbour reply, the attacker nodes are removed from the neighbour list. It improves the routing protocol security in MANETs. However, it increases the communication delay drastically. For reducing the delay of the cooperative bait detection algorithm, the harmony search algorithm is exploited in [18]. By utilizing the data routing information, the Black-hole attacks are identified using the Hybridization of Particle Swarm Optimization with the Genetic Algorithm (HPSO-GA) routing system in [19]. Using PSO and GA techniques, the HPSO-GA improves the security of MANET communication. When an interference causes between multiple routes, the HPSO-GA results in poor performance. In [20], the source node waits until it receives RREP packets from multiple nodes, after broadcasting the RREQ packet into the network. A first RREP packet is considered as the response from the Black-hole attacker, and the next RREP is accepted for the data forwarding. However, it is not adequate in all the scenarios. If a source node receives the genuine RREQ, it loses the shortest path, as per the suggested security mechanism. It increases the delay and reduces the communication efficiency. Moreover, it does not always protect the network from the Black-hole attackers.

An agent-based technique is proposed in [21] using Ant Colony Optimization (ACO) algorithm. It exploits the digital signature scheme, watchdog, and path rater techniques to avoid the impact of Black-hole attackers in MANETs. Without having the digital signature, the Black-hole attackers do not involve in the route discovery process. Moreover, by applying ACO over multiple RREP packets, the security scheme in [21] can successfully identify the attackers effectively. How ever, the malicious scenario increases the routing overhead and deteriorates routing performance. Security scheme in [20] utilizes the reliability factor in the detection of Black-hole attackers in MANETs. If the reliability factor is in confusion state, the fake RREQ is broadcast into the network for preventing the Black-hole attackers. However, it is not the capability of detecting the smart Black-hole attackers, where only the received data packets are dropped partially, but not entirely. Thus, it is essential to consider the entire characteristics of Black-hole attackers to avoid the impact of those attackers on MANET routing.

Liu et al. introduced a trust model for mobile Adhoc networks. This trust model uses both trust propagation and cryptography[22]. In the proposed trust model, every node is initially assigned a trust value. In this paper, the author aims to develop an important concept for establishing a dynamic and collaborative trust model for mobile Adhoc networks. Furthermore, it could be used to enhance the significant measure of trust in the routing of a message in MANET. The author discussed the concepts in this paper are generic. It does not rely on centralized control, any particular routing protocol or key distribution protocol. The proposed method does not need accurate time synchronization, authentication system or any complex hash chaining techniques. The proposed method easily integrates with the current routing protocol of the mobile Adhoc network. However, the proposed model does not restrict or modify the route maintenance behaviour or the route discovery of the underlying protocol.

In [23],author recommended an effort return based model. This model is maintaining and establishing a trusted route without any cryptography means in the Adhoc network for DSR protocol. In network, every node calculates a direct trust level for all immediate neighbours. For calculating trust information for concerning nodes, every node uses a reputation exchange protocol to share reputation. HashCash a CPU-cost function is used in this model to control the spread of trust reputations by limiting the generation of extravagant requests.

This paper[24] is based on a fuzzy dynamic programming theory. In which a Nobel trust management model FTDSR(fuzzy trusted dynamic source routing) is proposed. This protocol is used to discover a trustworthy path and mitigate attacks from malicious nodes. The performance of FTDSR is compared with DSR and TDSR. Results represent that, there is a remarkable improvement in network throughput, PDR and detection ratio for malicious nodes.

2.1 Problem Statement

Most of the conventional security mechanisms assume that the AODV routing protocol is affected by the single black hole attack. These works are inefficient while facing smart Black-hole attackers in the provision of secure wireless communication[31, 32]. It emphasizes the recent research on MANET security to focus on the entire features of Black-hole attackers and extend the conventional systems to mitigate these attacks in MANET. Moreover, it is essential to focus on secure communication without affecting the performance of the AODV routing protocol. In a wireless communication environment, the possibility of occurring the harsh channel condition such as network collisions is high. This impact on Black-hole attack detection is high because the packet dropping due to network collision makes difficulties in the security system[28, 29]. Hence, observing the packet loss rate with sufficient numbers of interactions is essential. For facing such a problem, the proposed scheme plans to integrate the direct and indirect measurement by considering the number of interactions as a weighting factor. Moreover, the entire features of Black-hole attacks such as hop count deviation, sequence number deviation, and routing behavior are considered. It improves the efficiency of the attack detection system in MANETs.

2.2 Contributions

The main contributions of the proposed Consensus Routing and Environmental DIscrete Trust (CREDIT) Based Secure AODV in MANETs are as follows.

1. The proposed CREDIT aims at detecting the Black-hole attacks as well as to improve the routing performance using Discrete and Consensus Trust Measurement.
2. The Discrete trust measurement formulates the routing behaviour and contextual information into benefit and cost metrics, as well as expresses the interactions between the nodes to measure the accurate trust value of a neighbouring node.
3. The consideration of the consensus-based trust value of its neighbouring nodes avoids the camouflage of malicious nodes under the background of less number of communication and improves the accuracy of trust.
4. The trust collected on consensus evidence from the decision-makers is measured using the importance degree to complete the collected trust preferences and to improve the accuracy of trust.
5. The performance of CREDIT is simulated using NS2, and several routing metrics are evaluated to prove its superiority in MANETs.

3 Overview of the Proposed Methodology

The MANET routing protocols have no techniques to detect the Black-hole attacks in default. This work extends the conventional trust measurement of MANET routing, which adopts only the routing behaviour observation to cope with the malicious activities, by incorporating the discrete and consensus-based trust measurement for formulating the secure intermediate router selection problem as a secure coalition formation. The extended protocol is named as CREDIT. To detect the Black-hole attacks, the CREDIT includes three components, such as Building Discrete Trust, Building Consensus Trust, and Aggregating Discrete and Consensus Trust. Figure 1 represents the block diagram of the proposed methodology.

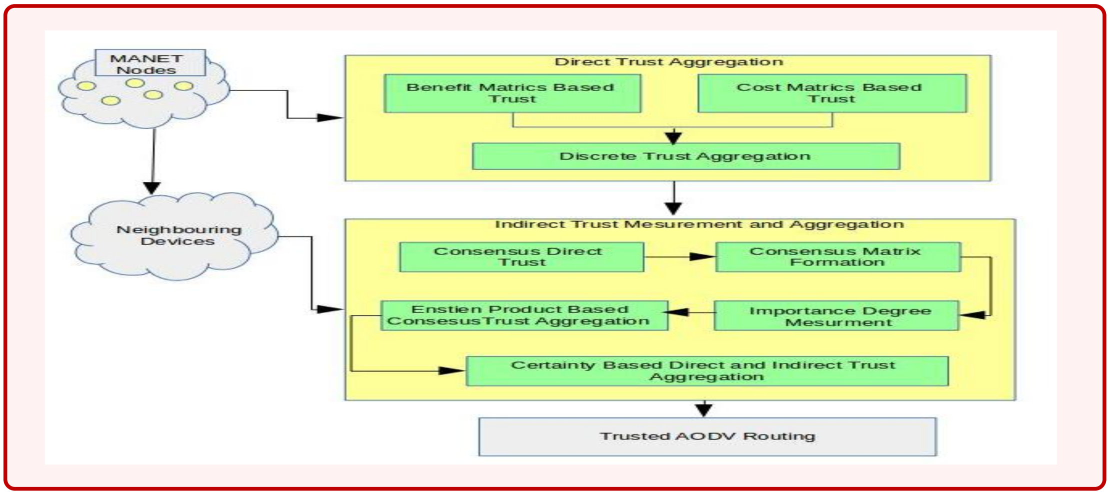

MANET Nodes
Direct Trust Aggregation
Benefit Matrics Based Trust
Cost Matrics Based Trust
Discrete Trust Aggregation
Neighbouring Devices
Indirect Trust Mesurement and Aggregation
Consensus Direct Trust
Consensus Matrix Formation
Enstien Product Based ConsesusTrust Aggregation
Importance Degree Mesurment
Certainty Based Direct and Indirect Trust Aggregation
Trusted AODV Routing

Fig. 1. Block Diagram of the Proposed Methodology

1. **Building Discrete Trust Model:** For modelling the trusted coalition of neighbouring nodes, the context attributes need to be of prime consideration in MANET routing. The contextual information for each node is discrete. If the routing nodes cooperate, the contextual information such as hop count deviation, and sequence number deviation are not of much help in the conventional MANET secure routing, as they assume that only the non-cooperative routing behaviour leads to losing more packets. Thus, the CREDIT builds the context information based discrete trust model against the Black-Hole attacks. The CREDIT divides the discrete trust parameters as benefit and cost parameters. The normalization among the discrete trust parameters provides the feasibility of adjusting the distribution of values and implementing a secure routing scheme on MANET against Black-Hole attack without degrading the trusted accuracy.
2. **Building Consensus Trust Model:** Although the discrete trust measurement is sufficient to observe both the routing behaviour and contextual information, the CREDIT may tend to incorrect classification of legitimate neighbours as malicious nodes. When the nodes have fewer interactions, the discrete trust alone is insufficient. Thus, the trusted coalition is built by a consensus level of neighbouring nodes trust on a particular node. Even though frequent message exchange between the nodes improves the certainty of discrete trust measure. Still, the discrete trust alone is inappropriate for wireless communication over MANETs.
3. **Aggregating Discrete and Consensus Trust:** To define the MANET trust aggregation in a new way for influencing the trusted coalition formation in the MANET, the CREDIT takes into account the certainty in discrete and consensus trust aggregation. The certainty denotes the number of interactions involved in trust measurement. The consensus trust value is taken into account concerning the level of certainty. It can balance the trust measurement accuracy and computational cost for trusted coalition formation.

Example : *The CREDIT incorporates Discrete and Consensus trust information. The Discrete parameters represent the specific characteristics of the Black-hole attacks, such as routing behaviour, hop count deviation, and sequence number deviation. The Consensus trust refers to the indirect trust value, collected from the neighbouring nodes. In order to evaluate the performance of CREDIT, the output is generated in each section by providing the sample input data. Considering the network model with randomly deployed sensor nodes of 15 in the square network area of 100m x 100m. The nodes are capable of communicating directly with others in the communication range of 25 m. The following figure shows the sample network topology with 15 nodes. Here, the Black-hole attacker is node 8.*

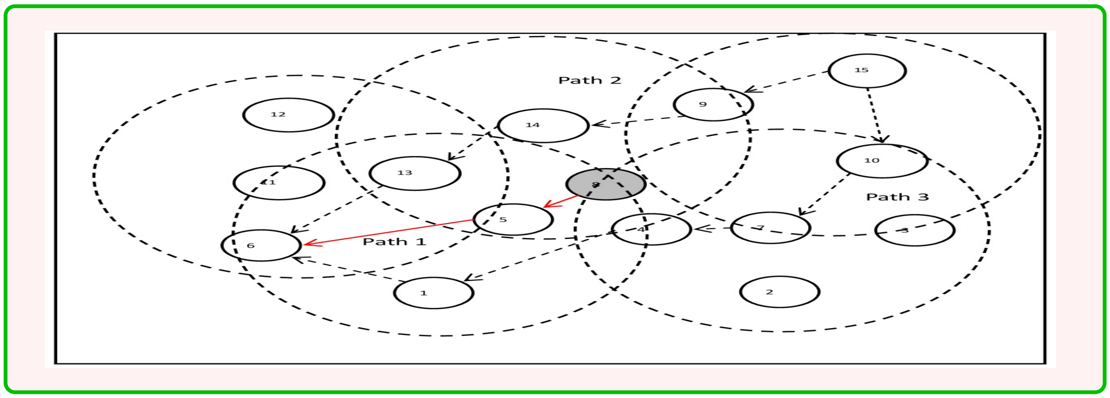


Fig. 2. Sample Network Scenario

From figure-2 The Black-Hole attacker 8 claims that it has the best route to the destination 15, but it does not have any route to the destination. The CREDIT is designed to restrict and detect the Black-Hole attacks in MANET. The trust measurement is built by the discrete trust as well as consensus trust collected from the neighbouring nodes.

Path between node 6 and 15	Intermediate Nodes	Hop Count	Destination Sequence Number
1	8,5	3	1000
2	13,14,9	4	2
3	1,4,7,10	5	2

Table 1. Path List

In table 1, the paths available between source (node 6) and destination(node 15) are listed along with its corresponding hop count and destination sequence number. The discrete trust measurement relies on the contextual information of a specific node. The contextual information is routing behaviour, hop count deviation, and sequence number deviation. The routing behaviour *is the benefit metric, whereas others are cost metrics. Table 2 represents the trust table of node 6.*

Neighbour Node of source 6	Routing Behaviour
1	.9
5	.85
11	.82
13	.96

Table 2. Trust Table of Node 6

The cost metrics denote the specific action of Black-hole attackers, since they exploit the smallest hop count, and the highest sequence number to launch the attack in MANET. The cost metric deviation is measured concerning the difference of hop count of a node from the maximum hop count of a neighbouring node for a particular destination. For sequence number deviation, the difference between the sequence number of a node and the minimum sequence number of a neighbouring node for a particular destination is considered. Table 3 represents the normalization of cost metrics of nodes.

First Intermediate Node in Various Paths	Hop Count	Hop Count Deviation	Destination Sequence Number	Destination Sequence Number Deviation
5	3	2	1000	998
13	4	1	2	0
1	5	0	2	0

Table 3. Normalization of Cost Metrics

3.1 Building Discrete Trust Model by using Benefit and Cost Parameters

The Black-Hole attacker claims that it has the best route to any node in MANET, but it does not have any route to the destination. The CREDIT is designed to restrict and detect the Black-Hole attacks in MANET. The design of fully distributed trust on MANET secure routing mandates that each node has to analyze the neighbour list in different perspectives from routing behaviour to contextual information. The trust measurement is built by the discrete trust as well as consensus trust collected from the neighbouring nodes. The discrete trust measurement relies on the contextual information of a specific node. The contextual information is routing behaviour, hop count deviation, and sequence number deviation. The routing behaviour is the benefit metric, whereas others are cost metrics. The cost metrics denote the specific action of Black-hole attackers, since they exploit the smallest hop count, and the highest sequence number to launch the attack in MANETs. The Cost metrics are measured only when a route reply packet is received through the neighbouring node. Notably, only the Benefit metrics denote the behaviour of a node, but the Cost metrics denote the trustworthiness of a route reply routed through a neighbour node. Thus, the Benefit metric based discrete trust is updated continuously, but the Cost metrics are maintained temporarily.

Normalization and Aggregation of Benefit and Cost Parameters in Discrete Trust Model:- Every node maintains the benefit and cost parameters in a list of the neighbouring nodes. The Cost metric value is zero until an RREP packet is received through the neighbouring node. The proposed CREDIT plans to normalize the parameters into a similar standardized format. In the attack detection process, normalization plays a crucial role. The data normalization is essential, especially when dealing with the parameters of different units. For example, the hop count deviation is a negative metric, and it uses the difference between the number of intermediate routers on a path. However, routing behaviour is a positive metric. The normalization of benefit parameter j of neighbouring nodes NH is done using the following equation. The neighbour list in node i and neighbouring nodes of node i are denoted using the NH and NH_i notation respectively. Where V_j represents the routing behaviour of a neighbour node in past transmissions, Min and max Vj represents the minimum and maximum value of V_j among all the neighbour nodes of NH_i respectively.

For Benefit Metrics[37][36].

$$BV_{NH_{ij}} \leftarrow \frac{V_{NH_{ij}} - min(V_j)_{NH_i}}{max(V_j)_{NH_i} - min(V_j)_{NH_i}} \tag{1}$$

Example :Calculation of Benefit metrics (Routing Behaviour) from table:-2. BV of node 1= (0.9-0.82)/(0.96-0.82)= 0.57; BV of node 5= (0.85-0.82)/(0.96-0.82)=0.214; BV of node 11= (0.82-0.82)/(0.96-0.82)=0; BV of node 13= (0.96-0.82)/(0.96-0.82)=1;

The normalization of cost parameters k of neighbouring nodes is done using the equation (2). Where Vk represents the hop count deviation and the sequence number deviation, which are observed from the recently received Route REPly (RREP) packets for a particular destination. During the route discovery process, the nodes that have a route to the particular destination replies to the source node with RREP packets. The RREP packet includes the hop count to reach the destination and sequence number. The cost metric deviation is measured concerning the difference of hop count of a node from the maximum hop count of a neighbouring node for a particular destination. For sequence number deviation, the difference between the sequence number of a node and the minimum sequence number of a neighbouring node for a particular destination is considered. If no neighbour node initiates the sending of RREP messages, there is no value for cost metrics in the neighbour list.

For Cost Metrics

$$CV_{NH_{ik}} \leftarrow \frac{max(V_k)_{NH_i} - NH_{ik}}{[max(V_k)_{NH_i} - min(V_k)_{NH_i}]} \tag{2}$$

Example :Calculation of Cost Metrics (Hop Count Deviation and Sequence Number Deviation) form table:-3.
*For Hop Count Deviation:-*CV of node 5= (2-2)/(2-0)= 0; CV of node 13= (2-1)/(2-0)=0.5; CV of node 1= (2-0)/(2-0)=1; *For Sequence Number Deviation:-*CV of node 5= (998-998)/(998-0)= 0; CV of node 13= (998-0)/(998-0)=1; CV of node 1= (998-0)/(998-0)=1;

The Discrete Trust metric (DT) is associated with the Benefit and Cost parameters. Based on the CREDIT, each node i estimates the discrete trust value DT on the neighbouring node NH_i(denoted as DT(i,NH_i)) using the following equation:

For Discrete Trust Metric,

$$DT(i, NH_i) \leftarrow \frac{[BV_{NH_{ij}}] + \sum_{i=1}^{k}(CV_{ij})}{(1+k)} \tag{3}$$

Example : *By fig:2, The Discrete Trust metric (DT) is measured for the one-hop neighbours, which forward the RREP packet for a destination node 15. Calculation of Discrete Trust metric for node 5,13,1 from above calculated value of respective benefit metric and cost metric. for The* $DT(i, NHi) are as follows: - DT of node 5 = 0.214 + 0 + 0/3 = 0.0713; DT of node 13 = 1 + 0.5 + 1 = 0.83; DT of node 1 = 0.57 + 1 + 1 = 0.856;$
However, the generic trust model without considering the contextual information is not compatible with the wireless scenarios. The benefit parameter value measurement is inadequate to conclude the routing behaviour of a node. However, packet loss also happens due to communication through a wireless medium. For the wireless nodes, it is insufficient to measure the direct trust with only the routing behaviour. The consideration of Cost parameter values is a benefit for observing the behaviour of Black-hole attackers exactly, the integration of Benefit and cost parameter values improves the efficiency of discrete trust measurement in MANETs.

3.2 Building Consensus Trust Model

The routing behaviour observation by a node is insufficient to confirm the presence of Black-hole attackers. However, it happens only after completing sufficient direct interactions. For the mobile nodes, it is inadequate to measure direct trust with limited communications. Thus, the trusted neighbouring nodes are considered as decision-makers. Concepts of MANET analysis are explained below in Definitions [35, 25, 26, 30].

Definition 1: In proposed CREDIT algorithm, the MANET is denoted as a directed graph G(D, E), with the nearby nodes representing decision-makers $D \in NH = 1, 2, 3, ...m$, Where $m \leq NH$ and edges E represents the wireless relationship between node i and decision-makers $\in NH$. The concepts in the MANET are formally described in the following definition.

Definition 2: An adjacent matrix $A = (DT(i, NH_i))m \times m$ is used to describe G(D, E). Where, $(d_i,\ d_j) = 1$ denotes that the d_i has trust value on a node d_j. Otherwise, there is no direct relation between the nodes d_i and d_j.

$$DT_{ij} = \begin{cases} 1, & (d_i, d_j) \in NH \\ 0, & (d_i, d_j) \notin NH \end{cases} \tag{4}$$

An adjacent matrix denotes whether the trust relationship between node i and decision-maker ∈ NH exists or not. However, trust strength is not measured. To solve this problem, the CREDIT proposes an adjacent weighted matrix. An adjacent weighted matrix is denoted using $A = (WDT_{ij})m \times m$,$d_{ij} \in [0, 1]$ denotes the trust strength of node i on node j.
An example scenario for the adjacent weighted matrix, associated with the directed MANET is illustrated in table 4. From table 4, the adjacent matrix is built.

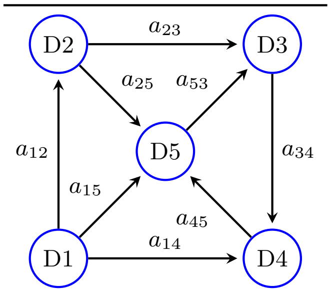


Table 4. A Weight Directed Graph

$$\text{A=}\begin{pmatrix} - & a12 & 0 & a14 & a15 \\ 0 & - & a23 & 0 & a25 \\ 0 & 0 & - & a34 & 0 \\ 0 & 0 & 0 & - & a45 \\ 0 & - & a53 & 0 & - \end{pmatrix}$$

Table 5. Sociometric

Definition 3: The sequence of edges(d_{i_1}, d_{j_2}), (d_{i_1}, d_{j_4}),(d_{i_1}, d_{j_5}), (d_{i_2}, d_{j_5}),(d_{i_4}, d_{j_5}), (d_{i_2}, d_{j_3}), (d_{i_3}, d_{j_4})——$(d_{i_{n-1}}, d_j)$ in Manet G(D,E) are called as trusted links between the decision makers, the trusted link from decision maker d_i to decision maker d_j is represented as $d_i \rightarrow d_j$.

In table4, The first five trusted links are used in estimating the discrete and consensus trust of node one on neighbouring node 5.
The weight is measured regarding importance degree. Due to the limitations of the wireless medium, it is difficult for the decision maker to provide a trust assessment on every neighbouring node. It tends to incomplete preferences and inefficient trust measurement in MANETs. To overcome this issue, the CREDIT plans to estimate the importance degree of every consensus trust value, which are provided by the decision makers.

Example : In Fig.3, The source node 6 measures the consensus trust on node 5 using the neighbouring nodes.

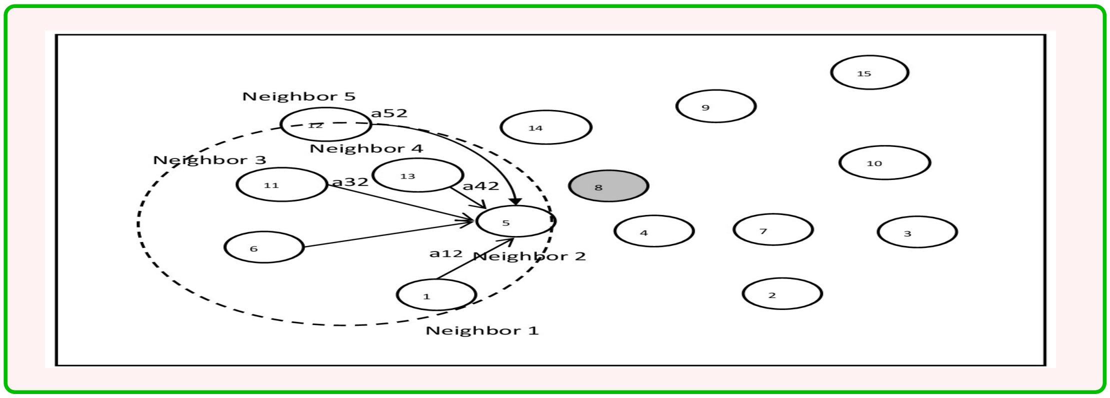


Fig. 3. Example Scenario for Consensus Trust Measurement

For the above example scenario, in fig: 3 there are five expert $a_{12}, a_{32}...a_{52}$ establish the trust relationship across a group in matrix. For figure the adjacent matrix is created, as follows.

$$\text{A=}\begin{pmatrix} - & a_{12} & 0 & - & - \\ 0 & - & - & 0 & - \\ 0 & a_{32} & - & - & - \\ 0 & a_{42} & 0 & - & - \\ 0 & a_{52} & - & - & - \end{pmatrix} \quad \text{A=}\begin{pmatrix} - & .85 & 0 & - & - \\ 0 & - & - & 0 & - \\ 0 & .9 & - & - & - \\ 0 & .62 & 0 & - & - \\ 0 & .95 & - & - & - \end{pmatrix}$$

Importance Degree Measurement The CREDIT estimates the incomplete preference values of a decision maker by preferences provided by other decision makers. The trust values of other decision makers reflect the importance of other decision makers' choices in the incomplete preference values estimation. The Importance Degree (ImD) is measured using the equations (4) and (5).

Definition 4: The in-degree centrality $C(d_k)$ of a trusted link of decision maker d_k is considered as:

$$C(d_k) \leftarrow \frac{1}{m-1} \sum_{1=1, i \neq k}^{m} C(d_{ik}) \tag{5}$$

Larger $C(d_k)$ represents higher ImD of d_k,it yield high over all degree trust in $d_k$among in group.

The in-degree centrality of a trusted link reflects the Importance Degree (ImD) of the decision maker in MANET.

$$ImD_k \leftarrow \frac{C(d_k)}{\sum_{i=1}^{m} C(d_{ik})} \tag{6}$$

Example: Applying the values from matrix of figure 3, the importance degree of each neighbour is identified. The in-degree centrality and Importance Degree are measured by for all the neighbouring nodes using the equations (5)and(6).

The in-degree centrality are measured for all the neighbouring nodes as follows:-

where $C(d_{15})$ is the in-degree centrality of a trusted link d_{15}. C(d) of 1 on 5 = (1/(5-1)) (0.9+0.62+0.95) = 0.615; C(d) of 2 on 5 = (1/(5-1)) (0.85+0.62+0.95) = 0.60; C(d) of 3 on 5 = (1/(5-1)) (0.85+0.9+0.95) = 0.675; C(d) of 4 on 5 = (1/(5-1)) (0.85+0.9+0.62) = 0.5921;

The importance degree are measured as follows:-

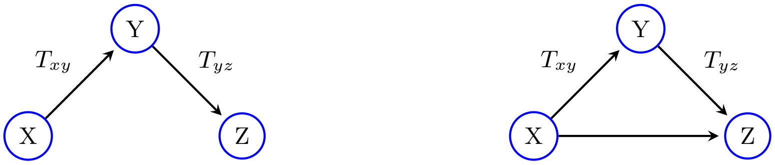
ImD 1 = 0.615/ (0.85+0.9+0.62+0.95) = 0.1852; ImD 2 = 0.60/ (0.85+0.9+0.62+0.95) = 0.1807; ImD 3 = 0.675/ (0.85+0.9+0.62+0.95) =0.2033; ImD 4 = 0.5921/ (0.85+0.9+0.62+0.95) = 0.178

The incomplete trust values are estimated by the preference of the most trusted decision-maker by the decision-maker who provides the incomplete trust value. In order to improve the trust consistency degree, it is essential to reduce the distance between the estimated trust value and the decision-makers' weighted preferences using the importance degree measurement.

3.3 Aggregating Discrete and Consensus Trust using Certainty Measurement

Although, integrating discrete and consensus trust is essential for improving the accuracy of Black-hole attack detection in MANETs, considering the number of communication (Com) is important for overall trust measurement. The CREDIT utilizes the certainty degree $1-(Com)^{-}1$, which denotes the confidence level of the discrete trust value, concerning the number of communications between the nodes. The confidence level on discrete trust is high when a high number of exchanges are processed. Notably, not only the malicious behaviour affects communication efficiency, but also the network constraints also affect the successful packet delivery. Thus, a large number of communication is essential to estimate an accurate trust value.

Definition 5: Considering the three nodes x,y,z where the node x and y do not have a number of interactions required for trust estimation. However, some information on whether or not node x can trust node z can still be inferred, based on transitivity. Therefore, it is necessary to design a mechanism to analyze whether an unknown expert can be trusted or not. The Einstein product is used as the triangular norm. The consensus trust is estimated by considering the general equation given below[27, 34, 39].



(a)No direct trust between X and Z (b)Trust propagation between between X and Z via Y

Table 6. Trust Propagation via Trust Path

The general Einstein Product is: $T(x, y) \leftarrow (x.y)/[1 + (1 - x)(1 - y)]$ *or* $T(x, y) \leftarrow (x.y)/[2 - (x + y - xy)]$. Where $x \in [0, 1]$ and $y \in [0, 1]$ are real number values.A function T is called a triangular norm (t-norm for short) if and only if it is commutative, associative, and monotonic [39].
T normal function for m argument is evaluated:

$$T(x_1, x_2, .., x_m) \leftarrow \frac{2\Pi_{i=1}^{m} x_i}{\Pi_{i=1}^{m}(2-x_i)+\Pi_{i=1}^{m} x_i}$$

Where $x_i \in [0, 1] \quad (i = 1, 2, .., m), T(x_1, x_2...x_n) \leq min(x_1, x_2...x_n)$.

Definition 6: A T is a mapping $T : [0, 1]^2 \rightarrow [0, 1]$ having following properties:

- Commutativity: T (x, y) = T (y, x)
- Monotonicity: $T(x_1, y_1) \geq U(x_2, y_2) if x_1 \geq x_2$ and $y_1 \geq y_2$
- Associativity: T(x,T(y,z)) = T(T(x,y),z)

.

Calculate Consensus Trust Measurement using Einstein Product:- CT represents the consensus trust value. The CT_{ij} is measured using the Einstein Product, as shown in equation (7). Moreover, the consideration of ImD maximizes the consistency degree.

$$CT_{ij} \leftarrow \frac{2\Pi_{j=1}^{m}(ImD_j * DT_{ij})}{\Pi_{j=1}^{m}(2 - (ImD_j * DT_{ij}) + \Pi_{j=1}^{m}(ImD_j * DT_{ij}))} \tag{7}$$

Example:-From above example and fig: 3, the node 6 determines the consesus trust on node 5 by consesus trust equation.
CT(6,5)=2(0.1852*0.85*0.1807*0.9*0.2033*0.62*0.178*0.95)/ (2-0.1852*0.85)(2-0.1807*0.9)(2-0.2033*0.62)(2-0.178*0.95)+ (0.1852*0.85*0.1807*0.9*0.2033*0.62*0.178*0.95)
= 0.0010913/(11.61+0.000545) = 0.000093992

Calculate Overall Trust Measurement:-In Equation (8), OT represents the overall trust value.

$$OT_{ij} \leftarrow ([1 - (Com)^{-1}]DT_{ij} + [1 - (1 - (Com)^{-1})]CT_{ij}) \tag{8}$$

A path is selected, only when a neighbour node attains high trust value due to the routed legitimate RREP packet. A highly trusted path is selected through the high trust neighbouring node. It reduces the impact of Black-hole attacks on routing efficiency, due to the consideration of Benefit and Cost metrics in the trust measurement. Thus, the Discrete and consensus-based trust evaluation in MANETs improves communication security without degrading the routing performance.

Example: Using the equation (7), the overall trust is measured. Considering that the communication between node 6 and 5 is 10. and OT(6,5) =1-(10)-10.85 + 1-(1-(10)-1)0.000093992
= 0.765 + 0.000009399; = 0.765009
Likewise, the OT value on nodes 1 and 13 are measured. Among them, a node 13 attains high trust value. Thus, path 2 in 2is selected for data routing. Moreover, node 5 receives less trust among them. So, the RREP initiator of node 8 is considered as a suspected node. Using the CREDIT methodology, the MANET can deliver the data packets successfully to the destination.

4 Performance Analysis

Performance Evaluation of the proposed algorithm (CREDIT) under the black-hole attack is implemented using the NS-2.35 network simulator[45]. Simulation has been performed for various cases like *Varying the normal number of nodes* and *Varying the number of attackers* . Furthermore, The proposed CREDIT algorithm is compared with the existing Enhanced AODV (EAODV)[16]. The CREDIT algorithm is a modification of AODV which is a standard and widely used routing protocol for wireless Adhoc networks. The performance evaluation is conducted over a randomly distributed mobile nodes, and the number of mobile nodes deployed in the network is set to 100. The nodes move with the maximum speed of 30m/s over an area of 600m x 600m and employing the IEEE 802.11 MAC protocol. The nodes can directly communicate with each others in the range of 200m. The CREDIT uses Constant Bit Rate (CBR) and User Datagram Protocol (UDP) in the application and the transport layer respectively. Performance Metrics and simulation environment7 has given below.

4.1 Performance Metrics and Simulation Result

(a)Performance Metrics: The following metrics are used to evaluate the comparative performance of proposed algorithm (CREDIT) under various test cases.

- **Throughput:**It denotes the rate of successful data delivery over the communication link in the network.

$$Throughput = \frac{(8 * TB)}{(TLBR - TFBS)}$$

Where, **TB** is Total Number of Bytes, **TFBS** is Time at First Bit was Sent and **TLBR** is Time at Last Bit Received
- **Packet Delivery Ratio Analysis** Packet Loss Rate in Manet is evaluated by Packet Delivery Ratio(PDR).
PDR is ratio of packet received by the destination with packet sent by the source.

$$PDR = \frac{P_r}{P_s} * 100$$

P_r are Received Packets and P_s are Sent Packets
- **End To End Delay** End To End Delay is defined as, time taken for transfer of packet from source to destination is called End To End Delay(EED).

$$EED = D_{trans} + D_{prop} + D_{proc} + D_{queuing}$$

Where
D_{trans} Transmission Delay, D_{prop} Propagation Delay
D_{proc} Processing Delay, $D_{queuing}$ Queuing Delay

- **Delay:** An average time taken by a packet to reach the destination.
- **Detection Accuracy:** It is the ratio of the number of accurately identified Black-hole attackers to the total number of Black-hole attackers in the network.

(b)Simulation Environment:

Simulation Environment

Simulation Parameter(s)	**Value(s)**
Simulation Area	600*600 square meter
Radio-Propagation Model	TwoRayGround
Physical Layer	802.11b
Antenna Model	OmniAntenna
MAC Layer	802.11
Routing Protocol	AODV
Transport Layer Protocol	UDP
Application Layer Protocol	CBR
Simulation Time	30sec
Mobility Model	Random way Point
Number of Mobile Nodes	100
Network Simulator Version	NS-2.35

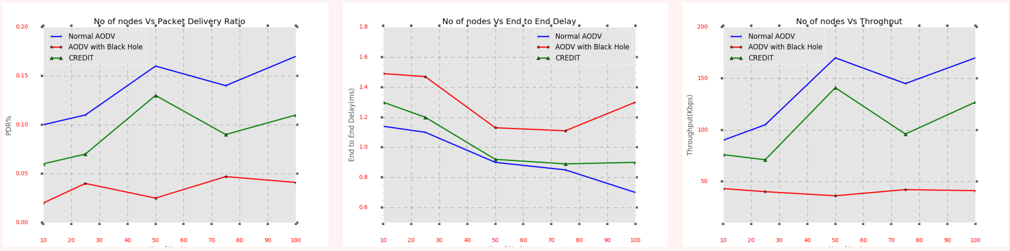
Table 7. Simulation Parameters

4.2 Simulation Result

***Test 1:* Varying Number of Nodes** In this test evaluation, simulation has been performed with varying no. of mobile nodes 10 to 100 in MANET. In addition, there is a single black hole node which is active in the network, which is performing a malicious activity like packet dropping. For performance evaluation, there are fixed parameters like PDR, Network Throughput and End to End Delay. Simulation results are illustrated regarding the following parameters are given below.

1. *Packet Delivery Ratio Vs No of Nodes:-* Figure: 4(a) shows the PDR result of normal AODV, AODV under black hole attack and proposed scheme CREDIT with varying no of nodes in the network environment. As a result, PDR decreases due to increasing the no. of nodes in the network. In addition, the figure is represented that normal AODV has the highest PDR% but in the presence of a single black hole node, PDR of AODV under black hole attack has dropped. This happened because there is no security mechanism has applied against the black hole attack. Along with the proposed algorithm CREDIT is employed. In the proposed mechanism, there is consideration of discrete and consensus trust along with number of communication performed between nodes. It leads to the detection of black-hole nodes and isolates them from the network. Therefore the result showed an improvement in the percentage of PDR from 0.04% to 0.08% as compared with AODV under the black hole environment.

2. *End to End Delay Vs Number of Nodes:-* In figure: 4(b) the result shows that there is the lowest EED of normal AODV as compared with AODV under black-hole attack that is 1.14 to 0.7. This happens due to the shortest path selection strategy applied to reach the destination. In addition, the result shows that EED increases rapidly under the malicious node attack in the network. because the malicious node is dropping the packet continuously. Along with the proposed algorithm CREDIT is employed. That leads to better results as compared to AODV under a black hole attack. In addition to the decrease in delay from 0.19ms to 0.4ms.As compared to the CREDIT algorithm with normal AODV, CREDIT has more end to end delay because of extra calculation and extra control packet needed to detect the suspicious malicious node.
3. *Throughput Vs Number of Nodes:-* In figure: 4(c) shows that there is highest throughput in normal AODV as compared with AODV under black-hole attack. Also Compare to the proposed trusted AODV CREDIT scheme with AODV under black-hole attack, the result represents the improvement of throughput from 33kbps to 84kbps in varying no of nodes environment. Proposed Scheme CREDIT is a more effective scheme for detecting the malicious nodes before data transmission in the network.



(a) Packet Delivery Ratio Vs No of Nodes

(b) End to End Dealy Vs No of Nodes

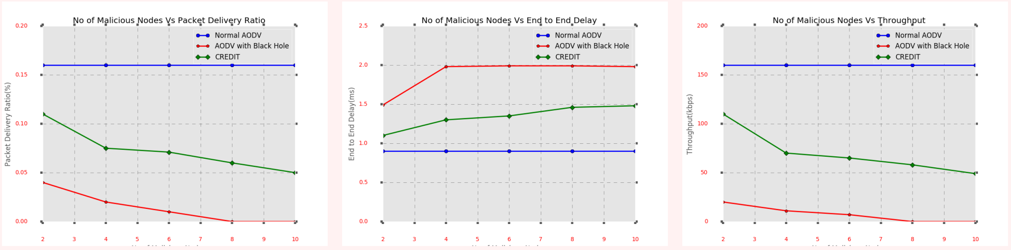
(c) Throughput Vs No of Nodes

Fig. 4. Varying No off Nodes.

Test 2: **Varying the Number of Malicious Nodes** Simulation is performed for varying the attacker's nodes from 2% to 10% with randomly distributed normal mobile nodes set up to 100 in the network environment along with fixed performance matrix parameters. The conclusion of simulation is showed in the form of graphs.

1. *Packet Delivery Ratio Vs Number of Malicious Nodes:-* In figure: 5(a) represents that PDR% decreases when the percentage of malicious node increased. PDR% is decreased because of increased packet dropping activity done by various malicious nodes. Furthermore, it is observed that the proposed CREDIT scheme improves much better PDR% under the black hole attack. But compare with normal AODV, it is also decreased i.e 0.038 to 0.09. Also, the figure shows PDR nearly zero in AODV with a black-hole attack when multiple malicious nodes are active in the network.
2. *End to End Delay Vs Number of Malicious Nodes:-* In figure: 5(b) shows the EED results of Proposed CREDIT Mechanism, normal AODV and AODV under black-hole attack by varying attackers from 2% to 10%.In addition, it is observed that a highly vulnerable environment creates a high EED. The proposed scheme presents better results in terms of EED under various malicious nodes environments.

3. *Throughput Vs Number of Malicious Nodes:-* From the figure: 5(c) it is observed that the throughput of CREDIT is always high when compared to AODV under black-hole attack. The selection of a most trustworthy path in CREDIT to deliver the data packets to the destination, it enhances the rate of delivered packets so throughput increases. The attacker drops all packets. From the figure, it is also observed that the throughput of AODV against multiple malicious nodes is nearly zero because of a lot of packet drops.



(a) Packet Delivery Ratio Vs No of Maliciuos Nodes (b) End to End Dealy Vs No of Maliciuos Nodes (c) Throughput Vs No of Maliciuos Nodes

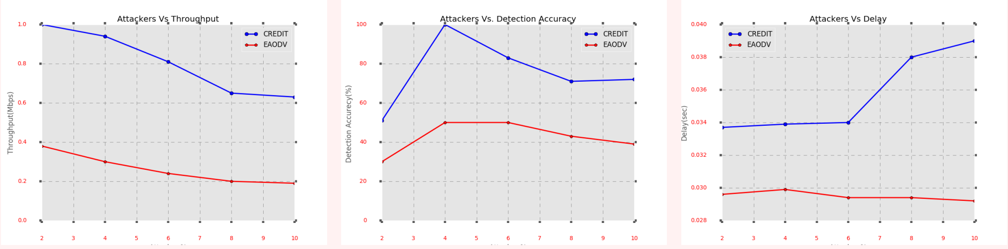
Fig. 5. Varying No of Malicious Nodes.

***Test 3:* Comparative performance Analysis of CREDIT with existing EAODV Protocol** The proposed CREDIT is compared with the existing Enhanced AODV (EAODV)[16]. The total simulation time is the 30s. To compare the performance of CREDIT and EAODV, the number of Black-hole attackers is varied from 2% to 10%. This scenario builds low to the high threat environment.

1. *Attackers Vs. Throughput:-* From figure 6(a), it is observed that the throughput of CREDIT is always high when compared to the existing EAODV. The attack detection accuracy is directly proportional to the network throughput. The selection of a most trustworthy path in CREDIT to deliver the data packets to the destination enhances the rate of delivered packets. However, the EAODV assumes that all the collected trust information from the neighboring nodes are always trustworthy. However, this is imperfect with the case of intelligent malicious activities. The CREDIT improves the throughput by 65% compared to that of EAODV with 100 node topology and 2% of attackers in the network. The proposed scheme takes into account the discrete and consensus-based trust information to improve the efficiency of the defence system. Moreover, the measurement of importance degree also ensures the accuracy of consensus-based trust aggregation even under a highly vulnerable environment. The CREDIT improves the throughput by 72.1% compared to that of EAODV with 100 numbers of node topology and 10% of attackers in the network.
2. *Attackers Vs. Detection Accuracy:-* In figure 6(b) shows the detection accuracy of CREDIT and EAODV, by varying the number of attackers from 2% to 10%. The consideration of discrete and consensus trust along with the number of communication performed between two nodes has to lead to a higher detection accuracy in CREDIT. Beyond the point of 4% of attackers, the detection accuracy of CREDIT starts to degrade moderately. The cost metric may be compensated when a Black-hole attacker assigns sequence number with the smallest deviation, and the actual hop count between the source and destination is also small. In such cases, the CREDIT experiences a moderate reduction in detection accuracy. The observed

influence of the number of attackers on the detection accuracy of the CREDIT is reasonable, compared to the existing EAODV. Beyond 4% of malicious nodes, the detection accuracy of CREDIT gets reduced from 100% to 70%, but it performs well in comparison with EAODV. Figure demonstrates that when the number of attackers is increased, the difference between the detection accuracy of EAODV and CREDIT with 100 node topology is relatively low. Because the EAODV takes into account the reputation aggregators and attempts to reduce the false-positive rate. However, huge numbers of unnecessary control packets reduce the efficiency of EAODV. For instance, with 6% of attackers, both the CREDIT and EAODV attain nearly 83% and 50% of detection accuracy respectively.

3. *Attackers Vs. Delay:-* In figure 6(c) shows the delay results of CREDIT and EAODV by varying the attackers from 2% to 10% with 100 numbers of nodes in the environment. From figure , it is observed that the highly vulnerable environment creates a high delay in the CREDIT. A huge number of control packets increase the chance of network collision in the network and reduce the packet delivery ratio of EAODV. Thus, it reduces the packet delivery delay of EAODV. Although the throughput of CREDIT is greater than that of EAODV in all the environments, it can deliver the data packets in a considerable amount of delay. With the help of certainty factor and importance degree, the CREDIT attempts to reduce the impact of false alarm rate as well as decide the behaviour certainty on nodes using benefit and cost metrics. From figure 5, the packet delivery delay of CREDIT increases by 0.0054 sec while increasing the percentage of attackers from 2% to 10%, due to the impact of undetected Black-hole attackers. The EAODV drops the throughput by more than 25% from low to the high threat environment. So it reduces the delay from 0.0296 sec to 0.0292 sec while increasing the attackers.



(a) Attackers Vs. Throughput (b) Attackers Vs. Detection Accuracy (c) Attackers Vs. Delay

Fig. 6. Varying No of Nodes.

5 Conclusion

This work presented a trust-based defence system against the Black-hole attackers in MANET. The proposed CREDIT considered the Discrete and Consensus Trust in identifying and isolating the Black-hole attackers from the network. It has demonstrated the accurate detection of Black-hole attackers and efficient packet delivery capability of CREDIT in the presence of 2% to 10% of Black-hole attackers in the network. The usage of Benefit and Cost metrics in discrete trust measurement prevents the inaccurate trust measurement due to dynamic network conditions without increasing the routing overhead. The consideration of the certainty factor in the integration of discrete and consensus trust values decides the dynamic weight for those trust values and improves the accuracy of trust measurement against the Black-hole attackers. Since there is a possibility of fake trust exchanges, the importance degree is measured for every evidence provider. Thus, the CREDIT can detect the Black-hole attackers, even if fewer interactions are performed between the nodes. The evaluation of CREDIT protocol shows the improved detection accuracy of the Black-hole attackers by nearly 70% even under a highly vulnerable MANET environment, compared to the existing EAODV.

6 Limitations and Future Work

This work may extend the conventional trust measurement of MANET routing, which adopts only routing behaviour observation to cope with malicious activity. In addition, performance evaluation of proposed work under Black-hole attack has not been performed for varying the mobility of nodes in terms of speed. Furthermore, various performance metric parameters like routing overhead, Normalized Routing Load (NRL), route discovery latency and malicious discovery ratio which can be added for examine the performance of protocol in presence of malicious nodes. This limitation may be considered in future work for extension of protocol for better and efficient results.

This work can also be extended for securing some more reactive routing protocol except AODV. Further more, the proposed algorithm can also focus on providing detection accuracy of malicious nodes using a suitable and effective statistical method.

References

1. Chlamtac, I., Conti, M. and Liu, J.J.N., 2003. Mobile ad hoc networking: imperatives and challenges. Ad hoc networks, 1(1), pp.13-64.
2. Al-Shurman, M., Yoo, S.M. and Park, S., 2004, April. Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual Southeast regional conference (pp. 96-97). ACM.
3. Cai, J., Yi, P., Chen, J., Wang, Z. and Liu, N., 2010, April. An adaptive approach to detecting black and gray hole attacks in ad hoc network. In 2010 24th IEEE International Conference on Advanced Information Networking and Applications (pp. 775-780). IEEE.
4. Perkins, C., Belding-Royer, E. and Das, S., 2003. Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).
5. Furht, B. and Ilyas, M. eds., 2003. Wireless Internet Handbook: Technologies, Standards, and Applications. CRC Press.
6. Royer, E.M. and Toh, C.K., 1999. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Commun., 6(2), pp.46-55.
7. Esmaili, H.A. and Shoja, M.R., 2011. Performance analysis of AODV under black hole attack through use of OPNET simulator. arXiv preprint arXiv:1104.4544.
8. Govindan, K. and Mohapatra, P., 2011. Trust computations and trust dynamics in mobile adhoc networks: A survey. IEEE Communications Surveys & Tutorials, 14(2), pp.279-298.
9. Singh, S. and Bajpai, A., 2016. A Survey on Black Hole Attack in MANET. In Proceedings of the international conference on recent cognizance in wireless communication and image processing (pp. 933-941). Springer, New Delhi.
10. Tseng, F.H., Chou, L.D. and Chao, H.C., 2011. A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), p.4.
11. Jain, S. and Khunteta, A., 2015, March. Detection techniques of blackhole attack in mobile adhoc network: A survey. In Proceedings of the 2015 international conference on advanced research in computer science engineering and technology (ICARCSET 2015) (p. 47). ACM.
12. Nadeem, A. and Howarth, M., 2013. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. Telecommunication Systems, 52(4), pp.2047-2058.

13. Wu, B., Chen, J., Wu, J. and Cardei, M., 2007. A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless network security (pp. 103-135). Springer, Boston, MA.
14. Gurung, S. and Chauhan, S., 2018. A dynamic threshold based approach for mitigating black-hole attack in MANET. Wireless Networks, pp.1-15.
15. Noguchi, T. and Hayakawa, M., 2018, August. Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 539-544). IEEE.
16. Yaseen, Q.M. and Aldwairi, M., 2018. An Enhanced AODV Protocol for Avoiding Black Holes in MANET. Procedia Computer Science, 134, pp.371-376.
17. Fahad, A.M., Ahmed, A.A., Alghushami, A.H. and Alani, S., 2018, October. Detection of Black Hole Attacks in Mobile Ad Hoc Networks via HSA-CBDS Method. In International Conference on Intelligent Computing and Optimization (pp. 46-55). Springer, Cham.
18. Yasin, A. and Abu Zant, M., 2018. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Wireless Communications and Mobile Computing, 2018.
19. Thanuja, R. and Umamakeswari, A., 2018. Black hole detection using evolutionary algorithm for IDS/IPS in MANETs. Cluster Computing, pp.1-13.
20. Koujalagi A (2018) Utilization of edge position for digital image watermarking using discriminant analysis. Am J Compt Sci Inform Technol Vol.6
21. Panda, N. and Pattanayak, B.K., 2018. Energy aware detection and prevention of black hole attack in MANET. International Journal of Engineering and Technology (UAE), 7(2.6), pp.135-140.
22. Liu, Z., Joy, A.W. and Thompson, R.A., 2004, May. A dynamic trust model for mobile ad hoc networks. In Proceedings. 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2004. FTDCS 2004. (pp. 80-85). IEEE.
23. Pirzada, A.A., Datta, A. and McDonald, C., 2004, May. Propagating trust in ad-hoc networks for reliable routing. In International Workshop on Wireless Ad-Hoc Networks, 2004. (pp. 58-62). IEEE.
24. Xia, H., Jia, Z., Ju, L. and Zhu, Y., 2011. Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory. IET wireless sensor systems, 1(4), pp.248-266.
25. Dong, Y., Zha, Q., Zhang, H., Kou, G., Fujita, H., Chiclana, F. and Herrera-Viedma, E., 2018. Consensus reaching in social network group decision making: Research paradigms and challenges. Knowledge-Based Systems, 162, pp.3-13.
26. DONG, Yucheng, et al. Managing consensus based on leadership in opinion dynamics. Information Sciences, 2017, 397: 187-205.
27. Gassert, H., 2004. Operators on fuzzy sets: Zadeh and Einstein. In Seminar paper.
28. Gupta, P., Goel, P., Varshney, P. and Tyagi, N., 2019. Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET. In Smart Innovations in Communication and Computational Sciences (pp. 271-279). Springer, Singapore.
29. Hallani, H. and Shahrestani, S.A., 2008, November. Trust assessment in wireless ad-hoc networks. In 2008 1st IFIP Wireless Days (pp. 1-5). IEEE.
30. Kamis, N. H., Chiclana, F., and Levesley, J. (2018). Preference similarity network structural equivalence clustering based consensus group decision making model. Applied Soft Computing, 67, 706-720.
31. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N. and Jamalipour, A., 2007. A survey of routing attacks in mobile ad hoc networks. IEEE Wireless communications, 14(5), pp.85-91.
32. Kim, J. T., Kho, J. H., Lee, C. Y., Lee, D. W., Bang, C. S., Lee, G. (2008, August). A safe AODV (Ad hoc on-demand distance vector) security routing protocol. In 2008 International Conference on Convergence and Hybrid Information Technology (pp. 115-118). IEEE.
33. Ngai, E.C. and Lyu, M.R., 2004, March. Trust-and clustering-based authentication services in mobile ad hoc networks. In 24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings. (pp. 582-587). IEEE.
34. Victor, P., Cornelis, C., De Cock, M., & Herrera-Viedma, E. (2011). Practical aggregation operators for gradual trust and distrust. Fuzzy Sets and Systems, 184(1), 126-147.
35. Wu, J., Xiong, R., & Chiclana, F. (2016). Uninorm trust propagation and aggregation methods for group decision making in social network with four tuple information. Knowledge-Based Systems, 96, 29-39.

36. Xu, X.H., Du, Z.J., Chen, X.H. and Cai, C.G., 2019. Confidence consensus-based model for large-scale group decision making: A novel approach to managing non-cooperative behaviors. Information Sciences, 477, pp.410-427.
37. Xu, Z. (2009). An automatic approach to reaching consensus in multiple attribute group decision making. Computers and Industrial Engineering, 56(4), 1369-1374.
38. Yau, P. and Mitchell, C.J., 2003, July. Security vulnerabilities in ad hoc networks. In The Seventh International Symposium on Communication Theory and Applications, July 13?18, 2003, Ambleside, Lake District, UK (pp. 99-104).
39. Zhang, H., Palomares, I., Dong, Y. and Wang, W., 2018. Managing non-cooperative behaviors in consensus-based multiple attribute group decision making: An approach based on social network analysis. Knowledge-Based Systems, 162, pp.29-45.
40. Chandan, R.R., Kushwaha, B.S. and Mishra, P.K., 2018. Performance Evaluation of AODV, DSDV, OLSR Routing Protocols using NS-3 Simulator. International Journal of Computer Network and Information Security, 10(7), p.59.
41. Kushwaha, B.S. and Mishra, P.K., 2016. Comprehensive Analysis of Ad Hoc Network Routing Protocols. International Journal of Computer Applications, 139(3), pp.1-5.
42. Kushwaha, B.S. and Mishra, P.K., 2016. Different Traffic Patterns Over Ad Hoc Network Routing Protocols. International Journal of Computer Applications, 138(11), pp.1-5.
43. Chandan, R.R. and Mishra, P.K., 2018. A Review of Security Challenges in Ad-Hoc Network. International Journal of Applied Engineering Research, 13(22), pp.16117-16126.
44. Chandan, Radha Raman and Mishra, P.K., Performance Analysis of AODV under Black Hole Attack (March 12, 2019). Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE) 2019. Available at SSRN: https://ssrn.com/abstract=3351038 or http://dx.doi.org/10.2139/ssrn.3351038
45. The Network Simulator-NS-2.35. https://www.isi.edu/nsnam/ns/.