I. J. Computer Network and Information Security, 2018, 4, 48-64
Published Online April 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.04.06

Intelligent Energy Aware Fidelity Based On-Demand Secure Routing Protocol for MANET

Himadri N. Saha
Institute of Engineering & Management, Kolkata, India
E-mail: contactathimadri@gmail.com

Prachatos Mitra
Institute of Engineering & Management, Kolkata, India
E-mail: prachatosmitra@gmail.com

Received: 31 October 2017; Accepted: 16 January 2018; Published: 08 April 2018

Abstract—Mobile Ad-Hoc Networks are very flexible networks, since they do not depend on any infrastructure or central authority. Due to this property, MANETs are highly ubiquitous in defense, commercial and public sectors. Despite the usage, MANET faces problems with security, packet drops, network overhead, end-to-end delay and battery power. To combat these shortcomings, we have proposed a new trust based on-demand routing protocol that can adapt to the specific energy conditions of nodes in a MANET. It uses the concept of fidelity which varies depending on packet drops. This fidelity is monitored through direct and indirect methods. The main aim of the protocol is to develop a model that considers both trust and battery power of the nodes, before selecting them as prospective nodes for secure transmission of data. With dynamic battery threshold calculations, the nodes make an intelligent choice of the next hop, and packet losses are effectively minimized. In addition to providing data origin authentication services, integrity checks, the proposed "Intelligent Energy Aware Fidelity Based On-Demand Secure Routing (IEFBOD)" protocol is able to mitigate intelligent, colluding malicious agents which drop packets or modify packets etc. that they are required to forward. New packets called report and recommendation have been used to effectively detect and eliminate these malicious nodes from a network. Our protocol has been compared to other existing secure routing protocols using simulation, and it displays improved performance metrics, namely high packet delivery fraction, low normalized routing load and low end-to-end delay.

Index Terms—Mobile Ad-Hoc Network, Trust Model, Fidelity, Energy efficiency, Secure Routing Protocol, Battery Threshold, Blacklist, Glomosim.

I. Introduction

In the last decade, mobility has developed as an important parameter for wireless networks. Mobile ad hoc networks fit exactly into this requirement of the society. MANETs do not face any problem while routing unless a node has moved out of range [28]. In that case, the node has to establish communication through intermediate nodes. This high dependency on intermediate nodes leads to data being vulnerable. Without any protection, the data can easily be eavesdropped by an unknown node, or the data can be intentionally dropped or modified, so as to disrupt the system. These malicious nodes need to be detected and eliminated from the network, so that unnecessary packet drops and delays can be decreased.

There are many secure routing protocols [6] which have been built by modification of some traditional protocols [2, 3, 4, 5, 20, 32]. In our on-demand secure protocol we attempt to effectively mitigate the attacks mentioned in [7]. The secure routing protocols found in literature [6] do not consider the battery life of the neighboring nodes and can be very power consuming. Therefore, it is possible that in a safe routing path, packets are dropped due to low battery power and the process has to be restarted. Therefore, it is necessary to consider security as well as energy parameters while designing a routing protocol for MANET.

The rest of the paper is organized as follows. In section 2, we review some of the existing secure routing protocols. In section 3, we present the IEFBOD protocol. In section 4 & 5, we present the concepts related to fidelity and the battery threshold calculation respectively. In section 6, we analyze the performance of the protocol against various attacks. In section 7, we present the simulation environment in Glomosim and the output. In section 8, we present the performance metrics used for evaluating IEFBOD and the comparison graphs. In section 9, we draw the conclusions and provide possible areas for future work.

II. Related Work

In this section we have reviewed some of the existing secure routing protocols for MANETs. We highlight the specific issues with the protocols that motivated us to propose a novel secure, energy aware protocol for on-demand routing in MANETs.

Several secure protocols have been proposed in literature that can handle the different categories of attacks mentioned in [6]. The proposed secure protocols can be broadly classified into four sections.

A. Basic Secure Routing Schemes

These protocols provide basic authentication services which guard against modification and replaying of routing control messages. In Secure Routing Protocol (SRP) [22], a keyed-hash message authentication code (HMAC) and secret key is shared between the source and the destination pair for authentication. However, in doing so, the protocol may suffer cache poisoning and wormhole attacks. In Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [31], TESLA keys are used for authentication of the sender and one-way hash chains for authentication of the hop counts. This protocol demands synchronized clocks and uses of these keys make the protocol computationally expensive. Secure Ad Hoc On-Demand Distance Vector (SAODV) [20] uses digital signatures for sender authentication and uses the same strategy as SEAD for authenticating hop counts. SAODV is susceptible to man-in-the-middle (MIM) attacks and it is possible that the private key of a node is visible to other nodes. ARAN [15] guarantees confidentiality with the help of digital signature, but it demands extra memory. Moreover, it doesn't use hop count, hence the path selected may not be optimal.

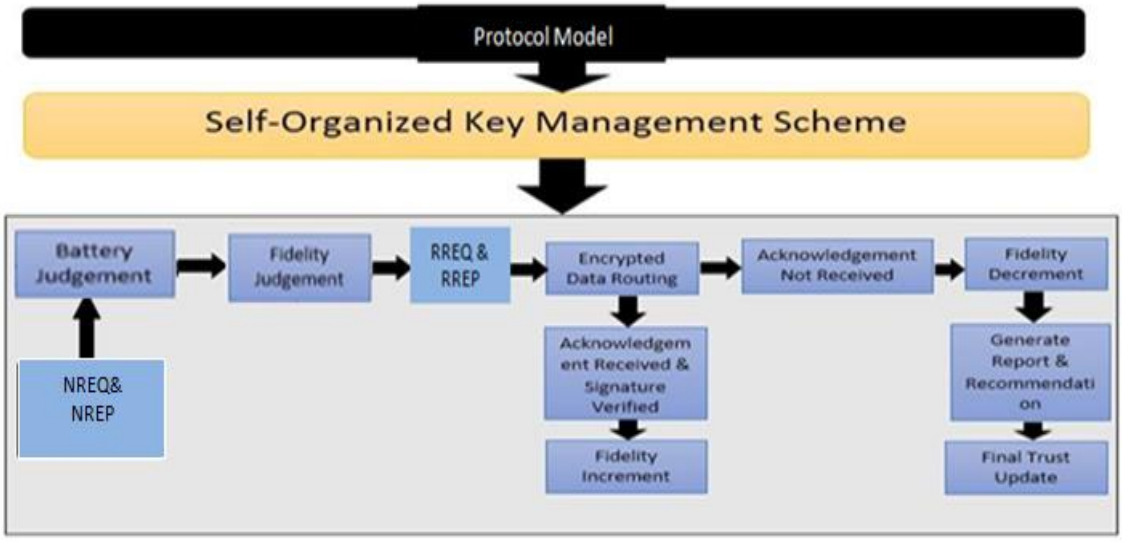


Fig.1. The Energy Aware Fidelity Based On-Demand Model

B. Trust based Routing Schemes

The trust-based routing schemes assign trust values based on the observed behavior of the nodes, through which a secure node is selected. Trusted Ad Hoc On-Demand Distance Vector (TAODV) [25] uses AODV protocol to provide anonymity for nodes in routing paths through encryption. It uses special packets to compute the trust value, but this incurs significant overhead. Fidelity Based On Demand Secure Routing Protocol (FBOD) [9] uses fidelity as a counter to assign trust values, through which information regarding the topology is obtained. However, it fails to consider blackmail attacks and does not consider the battery level.

C. Incentive based Schemes

The incentive-based schemes [15, 29] are implemented by assigning credits to nodes that cooperate and forward messages. The security model in [16] maintains nuglet counter which increases and decreases according to the node's behavior.

D. Schemes using Detection and Isolation Techniques

These schemes detect an attack and isolate it from the network, thereby decreasing the number of malicious nodes. For instance, Local Intrusion Detection (LID) [18] uses the node prior to the attacker node for intrusion detection, but it incurs a high end to end delay. In [24], the IDS and leader election methods are discussed. Here, if leader is compromised, then the whole system fails.

E. Our Contribution

Our contribution in this paper is to provide a secure and robust mechanism for establishing communication between network entities and to mitigate the effects of the malicious entities as presented in [7]. Robustness relates to successful communication within the nodes, i.e., successful sending and receiving of data packets. This is achieved by developing a cooperative routing algorithm which considers battery power as well as the activities of neighboring nodes in the past for routing. In addition, the proposed protocol attempts to detect malicious nodes by recommending them to other nodes in the network, ensuring they turn hostile to such malicious nodes and eventually eliminate them from the network. Most routing protocols for MANET do not consider both trust and energy parameters and some are vulnerable to common attacks. Via our IEFBOD protocol, we improve

upon the security issues highlighted in standard protocols and add the energy parameter to optimize robustness of the algorithm.

III. Proposed Protocol

In this section we discuss our protocol model and its (highlighted in Fig. 1). We have used a new self-organized key management system [8] that uses reduced memory space and makes the protocol lightweight.

The protocol is divided into seven stages that are each described in the subsection.

A. Neighbor Searching

Before a node can start routing packets to a destination, it has to identify its neighbors through neighbor searching. In MANETs, since the nodes move freely, neighbor searching has to be done frequently, by sending Neighbor Requests (NREQs) and receiving Neighbor Replies (NREPs), as acknowledgement from neighbors. The packet types are shown in Fig. 2. A node broadcasts the neighbor requests and waits for τ_1 = 2 * (Average delay) time for the neighbor reply packets to arrive.

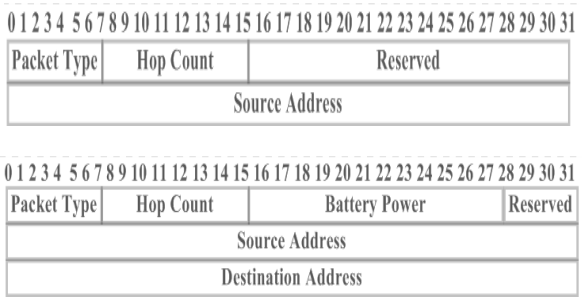


Fig.2. NREQ Packet Format (above) and NREP Packet Format (bottom)

If no NREP is received within τ_1 time, then the node keeps on sending the NREQ. The NREPs that are received are inserted into the Neighbor table, shown in Fig. 3. For new nodes, the fidelity is initialized as 0; otherwise the old fidelity is retained. The neighbor nodes also send their battery power through the NREP packets, which is used by the source node in the Battery Judgment stage. If the destination node is its immediate neighbor, then the route request is sent directly, after the Battery Judgment stage.

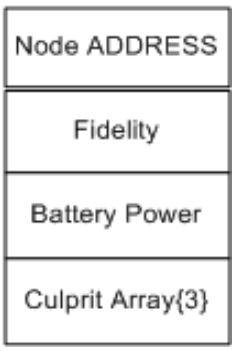


Fig.3. Data Structure for Neighbor Table

B. Battery Judgment

At this stage, the battery threshold for a neighbor node is calculated. Since at any instance, a neighbor node can either be an intermediate node or the destination node, we calculate two types of battery thresholds depending on the type of the node (explained in Section 5). In general, the battery threshold is calculated based on the packet sizes and the number of packets the neighbor node would have to send further for a successful data transmission. If the neighbor node has a battery value greater than or equal to the threshold, then the node is considered in the next stage, otherwise a new node is selected.

C. Fidelity Judgment

At this stage, a node selects the neighbor that has higher fidelity compared to that of other neighboring nodes. A high-fidelity value for a node indicates that it is has transmitted packets more dutifully than other nodes and can be considered trustworthy. The fidelity value for the involved node is increased by 1 for each successful transmission, and for failures, it is decreased by 1. This fidelity value can be incremented or decremented till a certain limit based on the battery power of the node, as explained in Section 4.

D. Sending and Receiving Route Request

The trustworthy node selected in the previous step is sent the route request (refer to Fig. 4). It waits for a certain time interval for the route reply to arrive. If the destination node is an immediate neighbor, it waits for τ_1 = 2 * (Average delay), otherwise, it waits for an interval of τ_2 = 2 * (Average delay) * (Network Diameter). In the worst case, the packet travels the entire Network Diameter.

As soon as the RREQ packet is received by a node, it becomes busy and caters solely to the origin node. This prevents loops and related attacks. The node also sends the 'fail array' in the RREQ packet, which contains the list of nodes which have failed to generate any route for a particular destination address. The nodes listed in the fail array are not selected for data transmission for the specific source-destination node pair. This helps in avoiding unnecessary delay. Let Node A in Fig. 6 send an RREQ packet with destination address E. Consider Node C is in the fail array. Node B will not send the RREQ to Node C, instead it will send it to Node D. Therefore, although the fidelity of C (Φ_{CB}) is more than that of D (Φ_{DB}) with respect to Node B, it is not selected as it is listed in the fail array.

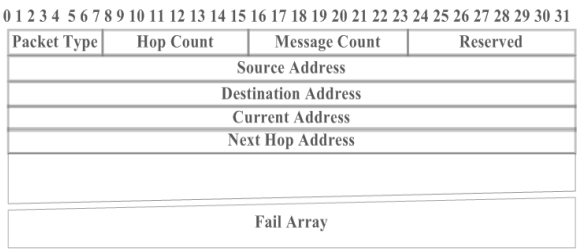


Fig.4. RREQ Packet Format

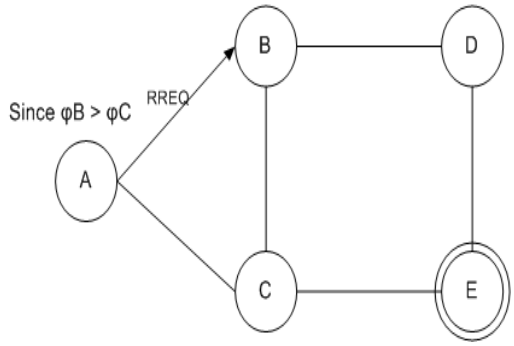


Fig.5. Node A sending RREQ to Node B

In case the RREQ times out, the origin node will move on and start selecting the next available node from the neighbor table. This node in turn repeats the process highlighted in this subsection until it gets the destination node in its neighbor table. If the neighbor table is exhausted, then the node repeats the process described above from the beginning. This is after a certain time interval which is the threshold.

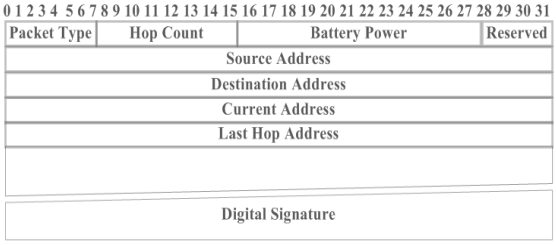


Fig.6. RREP Packet Format

Considering the example in Fig. 5, after the destination node has been discovered, the RREQ is sent to node E directly by node D. The RREP packet, as shown in Fig. 6, is sent back to the origin node through the same path. In Fig. 7, Node E (the destination node) will send the RREP back by digitally signing it. Node E will wait and stay busy for τ_3 τ_3 = 2* (MESSAGE_COUNT) * (AVG_DELAY) for the data packet to arrive.

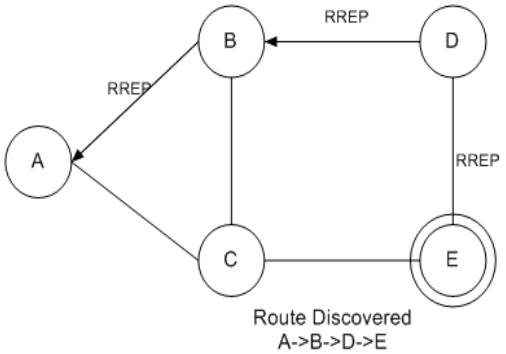


Fig.7. Node D sends RREP to Node A

E. Encrypting and Sending Data

Once the source node gets the route reply and verifies it, it prepares the data. The data packet is shown in Fig. 8. The data packets are sent from the same path through which the route reply came back. The source node encrypts the data with public key of the destination node and forwards it to the next hop. The intermediate nodes forward the data packet till it reaches the destination. Every node in this communication waits for a time interval τ_4 = 2* (HOP_COUNT) * (AVG_DELAY) for the ACK packet to arrive. In the situation highlighted in Fig. 8, the data will go from node A to E, via B and D nodes. Node A, B, D will have hop counts of 3, 2, 1 respectively; which signifies that τ_4 for Node A will be the greatest and for Node C will be the smallest.

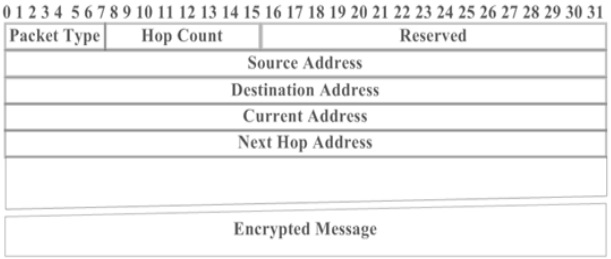


Fig.8. Data Packet

F. Acknowledgement Received

The Acknowledgement is generated only by the destination node, which is signed by the public key of the source. This allows the source node to ensure that the destination has received the data packet in a secured manner. The ACK packet is shown in Fig. 9. The nodes in the path increment the fidelity on receiving the ACK packet. Hence, in this case, the fidelity of node D with respect to B is incremented by 1, φ_{DE} =1, similarly $\varphi_{BA} = 1$. This route is then stored in the Route table. The route table can store only one entry. Therefore, if there are frequent transmissions to a particular destination node, then the route table can be used to retrieve the last path. This saves unnecessary packet requests.

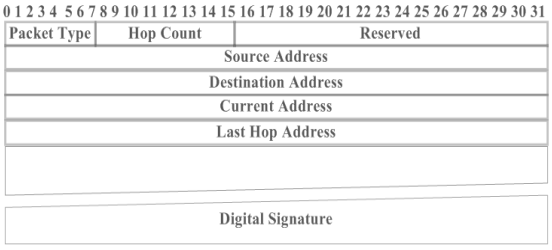


Fig.9. Acknowledgement Packet

G. Acknowledgement Not Received

If the ACK packet is not received by any of the intermediate nodes or source node within time τ_3, a node will assume that the communication is unsuccessful. The node will decrement its fidelity and for intermediate nodes, a Report packet is sent back to the previous hop. The Report packet, which is similar to RREP packet, is shown in Fig. 10. A node, on receiving a Report packet, decreases the fidelity of the node sending the Report in the data path. It generates a Report and sends it back to the last seen address, which continues till the source node. For instance, if Node B doesn't receive the ACK

packet within time from Node D, then Node B sends a Report Packet to Node A, and decreases the fidelity of node D by 1. In turn, Node A will decrease the fidelity of B by 1.

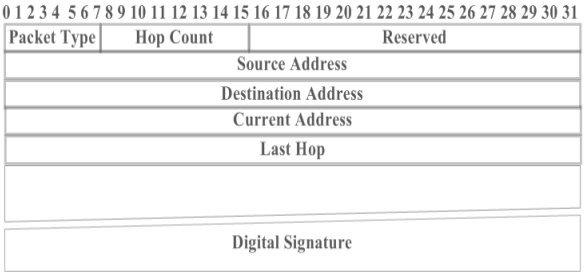


Fig.10. Report Packet

When acknowledgement is not received by a node within the time threshold, the node also prepares a recommendation packet with the name of the culprit and broadcasts it. The node which has encountered the culprit node will generate a recommendation for its other neighbor nodes in the network. The recommendation packet is shown in Fig. 11.

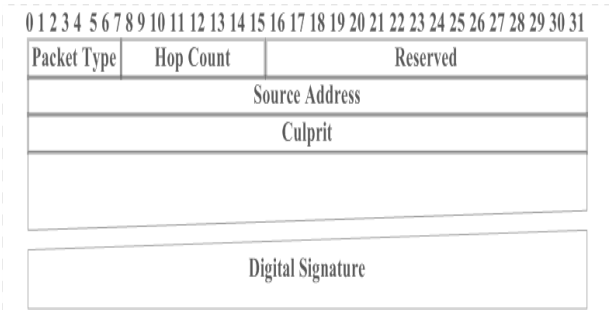


Fig.11. Recommendation Packet

On receiving a recommendation, any node will first decrement the fidelity of the recommended node by 1. When 3 such recommendations against the same node arrive from 3 different nodes, then the former is blacklisted and not used for further communication. Node B, in Fig. 8, will broadcast a Recommendation packet, against the culprit Node D, to all its neighbors. Node C will consider this recommendation packet, and decrease the fidelity of Node D. However, Node A, will not consider this recommendation packet, since it has already received information from Node B through the Report packet. So, a recommendation packet is only meant for the neighbors that were not associated with the specific data path.

The flowcharts for the protocols are shown in Fig. 12-18, which explain the data routing.

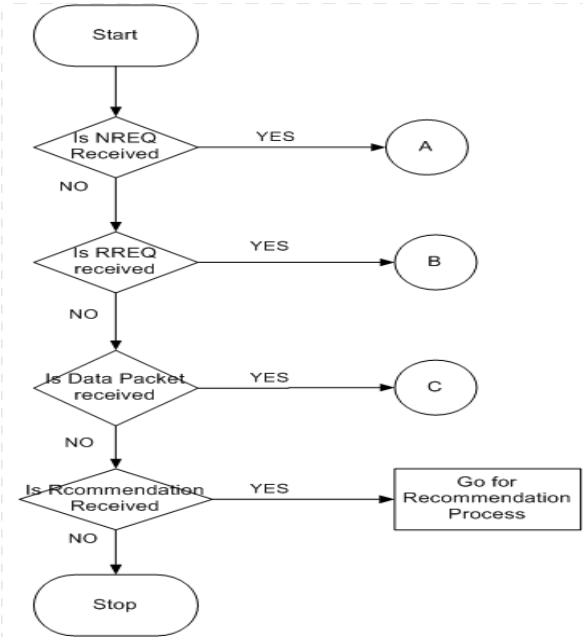


Fig.12. Flowchart for data routing in Sender Node

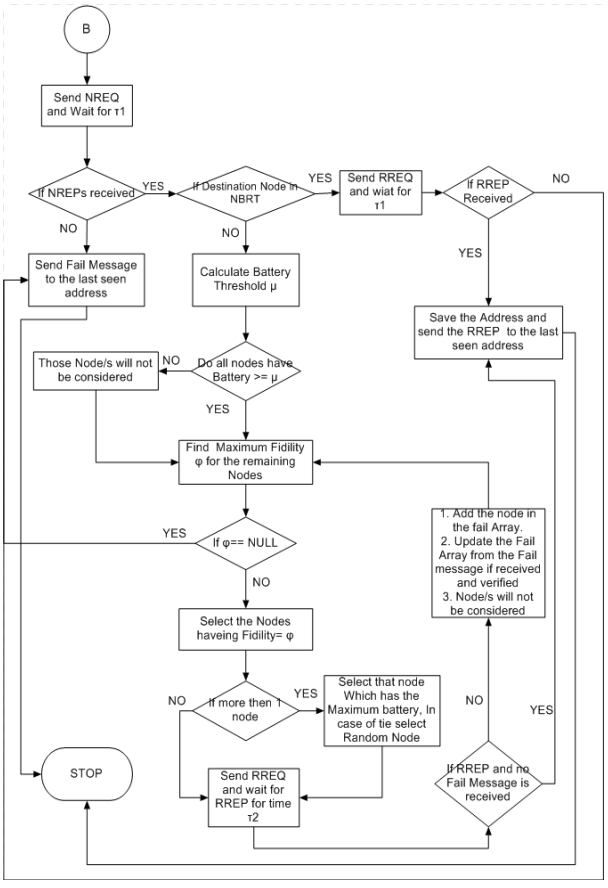


Fig.13. Flowchart for Intermediate Node

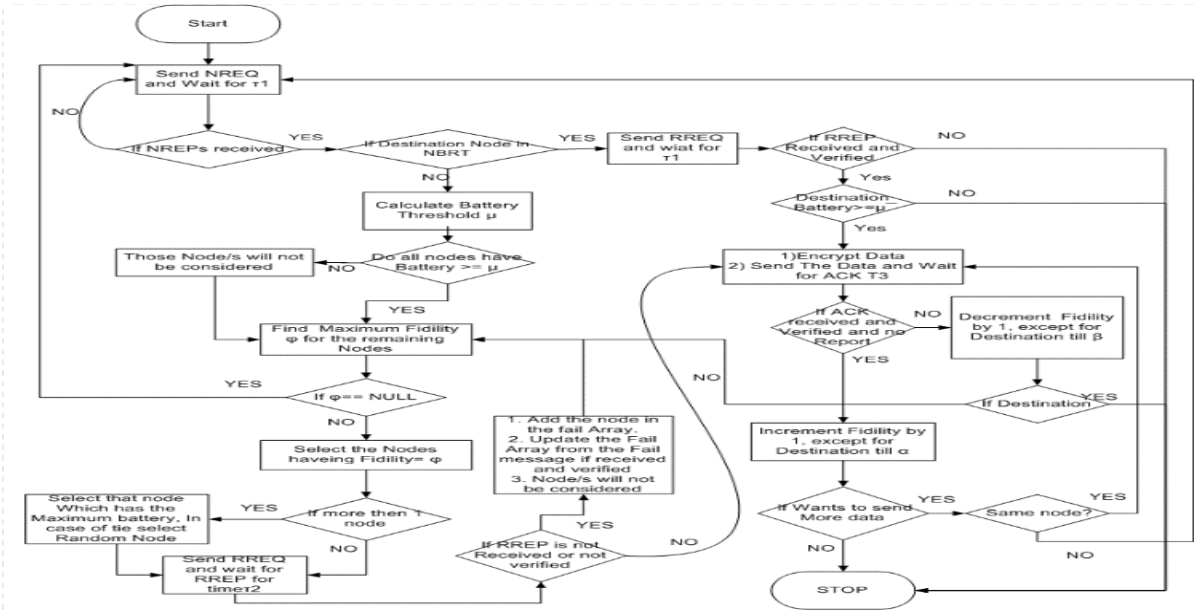


Fig.14. Flowchart for Intermediate Node- Section B

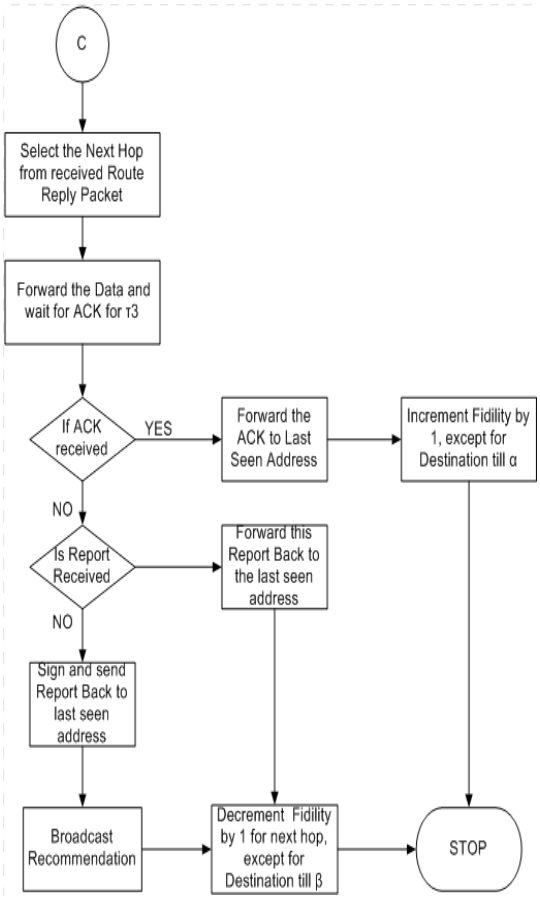


Fig.15. Flowchart for Intermediate Node- Section C

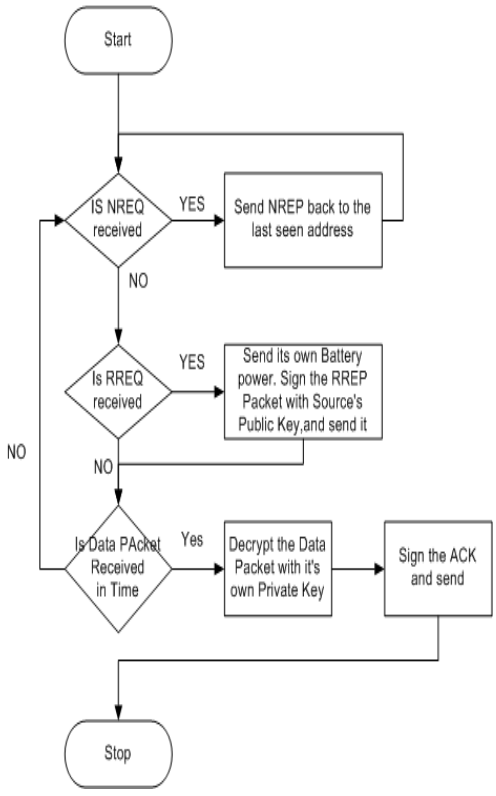


Fig.16. Flowchart for Destination Node

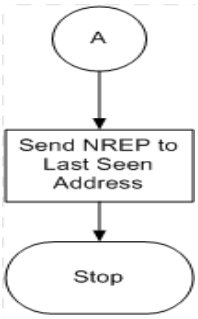


Fig.17. Flowchart for Intermediate Node - Section A

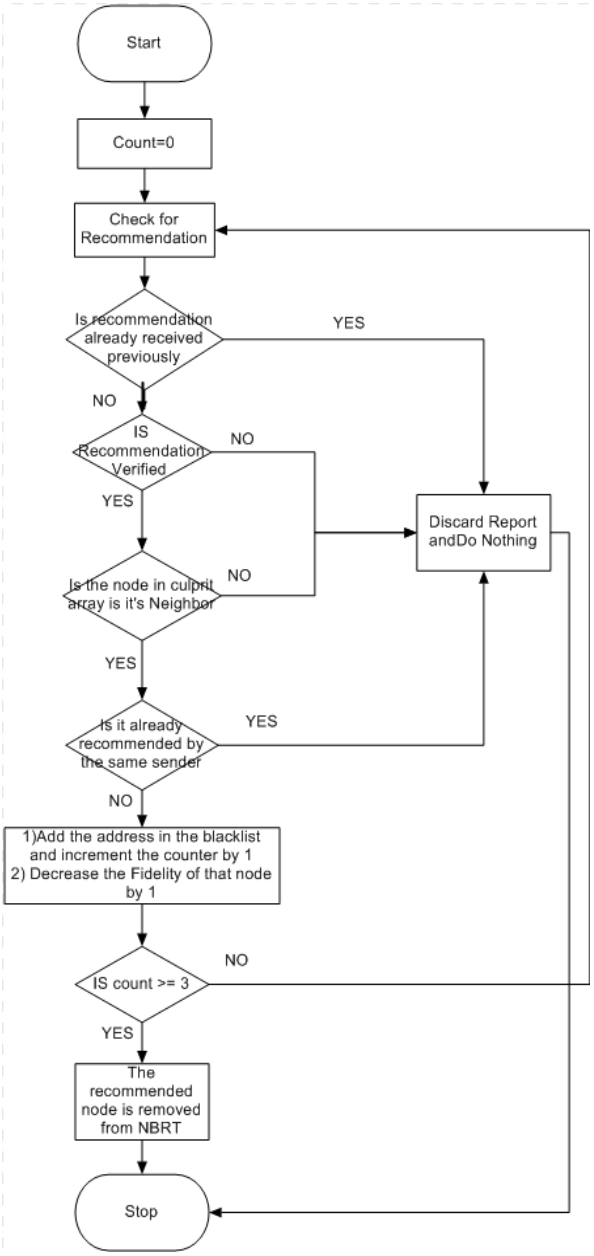


Fig.18. Flowchart for Recommendation System

IV. Fidelity Concepts

In this SECTION, we explain the concepts related to fidelity and the decisions associated with it. Fidelity is a measure of how much a node (say) A trusts its neighboring nodes (say) B and (say) C, with reference to selecting routes for transmission of a data packet.

Fidelity is only defined with reference to a specific node. For instance, consider that node B has a fidelity value $\varphi_{BA}\,\varphi_{BA}$ with respect to A, while C has a value $\varphi_{CA}\varphi_{CA}$ with respect to A. If $\varphi_{BA}\,\varphi_{BA} > \varphi_{CA}\varphi_{CA}$ then the data packet is transmitted via B to the next node. This methodology is utilized for selecting the routing path for each step, until the packet reaches the destination.

A. Types of Fidelity

We define two types of Fidelity for our model.

1. Direct Fidelity

Case 1

When a node A sends a data packet to its neighbor node B, the fidelity value of B with respect to A, $\varphi_{BA}\,\varphi_{BA}$ is incremented by 1 if B successfully transmits the packet. This is shown in Equation 1.

$$\varphi_{BA} := \varphi_{BA} + 1 \text{ on receiving ACK(A, B)} \quad (1)$$

Case 2

If a node A does not receive any acknowledgement for a data packet that it sent to its neighbor B, the fidelity value, φ_{BA}, of that neighbor is decreased by 1; as shown in Equation 2.

$$\varphi_{BA} := \varphi_{BA} - 1 \text{ on not receiving ACK(A, B)} \quad (2)$$

Case 3

In the third situation, consider that node A receives a report for some node D which is in the data path when packets are being transmitted via B. In this case, the fidelity value φ_{BA} is reduced as shown in Equation 3.

$$\varphi_{BA} := \varphi_{BA} - 1 \text{ on Report(A, B, D)} \quad (3)$$

Decreasing φ_{BA} potentially allows selection of some other neighboring node instead of node B, by node A. Therefore, in case node D is a malicious node intentionally dropping packets, it will eventually not be selected in the routing path. Hence, in general, the more secure path is selected.

2. Indirect Fidelity

Whenever a node A receives a recommendation (negative report) from a neighbor C about another neighbor B, A decreases the fidelity φ_{BA} and increases the counter of B by 1. This is show in equation 4.

$$\varphi_{BA} := \varphi_{BA} - 1,\ \text{count:=count+1 on REC(A, C, B)}] \quad (4)$$

A recommendation from a specific node is considered only once. In the proposed model, a node is blacklisted when its counter reaches 3, i.e. 3 neighbors recommend against it. The selection of the counter threshold is explained in Section 4B.

B. Counter Value

A counter for a node is incremented after each unique recommendation and when the count reaches 3, the node is blacklisted.

Selection of counter threshold:

We have observed that for count 3, the malicious nodes are effectively expelled from the network by the other nodes. To establish our claim, we performed 10 simulations to determine the average time required to expel a malicious node from a network, considering the count values as 1,3,5,7 and 9. We consider a network with uniform node placement and random waypoint mobility. The node traversal time T is set to 5ms.

We consider a single malicious node which has built a high fidelity in the network. Therefore, the malicious node is always selected over other nodes with lower fidelity. This particular situation is considered as in the other cases, the Report and Recommendations received causes fidelity to be decremented regularly, and the node is automatically not. Table 1 defines the time required by the network to eliminate a node after it commences its malicious behavior. This attack is similar to a gray hole attack. While selecting the counter threshold, we need to consider a) time efficiency in isolating the malicious node and b) minimum possible value that is optimal for the network (i.e. not too harsh). Since 1 or 2 recommendations cannot be considered due to the latter criteria, we choose count=3 as our threshold.

Table 1. Time Required (in ms) for Different Black List Counts and Number of Nodes

Count Nodes	1	3	5	7	9
10	125	425	650	875	1025
20	500	2125	3300	4600	5150
30	700	2750	4050	5800	6300

C. Fidelity Bounds

Since the battery powers of nodes are finite, fidelity cannot increase or decrease infinitely. Therefore, a node with high fidelity cannot be repeatedly selected. At some point, the battery of a node will drain, assuming there is no infrastructure for charging, and the node will be unable to send packets. Moreover, a high-fidelity node turning malicious (i.e. a Gray hole attack) can lead to severely reduction packet delivery in the protocol. Thus fidelity, φ, should be constrained to a range of values, and we can write $\varphi \in [\beta, \alpha]$. The calculation of β and α (i.e. the lower and upper bounds) is provided below:

Maximum Value:

We compute α, the maximum limit on Fidelity, with respect to battery required. Let us assume an ideal case for simplicity, with a single intermediate node between the source and destination which receives and forwards the packets. Consider that there are no malicious nodes. Let X be the initial battery power of the intermediate node in mAh, Y (refer equation 5) be the total power consumed for receiving & forwarding protocol packets for the initial connection establishment, (i.e. sending and receiving packets such as NREQ, NREP, RREQ, RREP), D be the total power consumed for each data packet in mAh and A be the total power for acknowledgement packet in mAh.

$$Y = P(NREQ) + P(NREP) + P(RREQ) + P(RREP) \quad (5)$$

The battery power will drain for each data reception & transmission; it will continue to drain till it becomes 0. After the initial connection establishment and data transfer the remaining battery power will be X-Y. The battery power consumed for each subsequent data transfer will be D+A. Therefore, the maximum number of times for data transfer (say M) is given by the ratio of these two quantities. So, the fidelity should increase till the battery power becomes 0; as shown in Equation 6.

$$\alpha = M_1 = \left\lfloor \frac{X-Y}{D+A} \right\rfloor \quad (6)$$

Thus, the maximum fidelity is dependent on the initial battery power (which is again device-dependent), as well as the powers consumed for data and protocol packets. This implies that the maximum fidelity value is essentially a device dependent value. By observing the results of a large number of data sets, it is seen that for 10 nodes and no malicious activity in the network, the maximum fidelity value achieved is around 4-5 before the battery is drained out. However, while increasing the no. of nodes to 20 leads to increase in fidelity value, no explicit relation between no. of nodes and fidelity threshold can be determined. Therefore, the maximum fidelity value can be empirically set to a certain level, but no definite relationship to obtain it can be established.

Minimum Value:

Initially the fidelity of a node is set to zero. The fidelity count can become negative due to a recommendation about the node or due to the node dropping packets. In either case, the fidelity count of the node will be negative. This fidelity can continue decreasing in the negative domain until the node does not have the battery power to start communication.

The minimum fidelity value β, can be found out by considering a situation where all the packets are dropped by a node, and hence the fidelity is decreased by 1. Considering the same parameters, X, D and A as in (6), we proceed with the calculation of the minimum value. In this case, Y = P(NREQ) + P(NREP) + P(RREQ). Consider for a node A, the only neighbor B is a malicious node. Initially, the fidelity of AB is 0, and each packet drop reduces it by 1. The reduction in fidelity value of B by A continues till it has battery power to transmit data. In the other possible scenario, if A has K neighbors, the fidelity of B is decremented K times; hence, the minimum value of fidelity count is the minimum of these two scenarios.

$$\beta = M_0 = \min\left(\left\lfloor \frac{X}{D+Y} \right\rfloor, -K\right) \quad (7)$$

Hence, the range for fidelity can be written as:

$$\min\left(\left|\frac{X}{D+Y}\right|, -K\right) \leq \varphi \leq \frac{X-Y}{D+A}$$

V. Battery Threshold Calculations

In this section, we calculate the battery thresholds. For this purpose, we have used a simulation model based on GloMoSim, detailed in Section 7.

The threshold battery charge for any intermediate and destination node, μ_i & μ_d respectively, are the minimum charges required to allow successive transmission and reception of data & protocol packets for a successful data transmission. These threshold values are used for making an intelligent decision during routing a packet, thereby adding a new dynamic to the system. This is calculated by the sending node during the neighbor discovery process. A source node computes both these thresholds μ_i & μ_d to decide if the immediate intermediate node or destination node has this minimum battery thresholds, to successfully carry on the communication. The battery values of intermediate and destination nodes are obtained through NREP and RREP respectively.

In our model, a node tries to pre-calculate the battery requirement of the next node for transmission. Whenever a node sends or receives a packet, it calculates the available energy by considering: (a) the specific Network Interface Card (NIC) characteristics, (b) the size of the packet and (c) the used bandwidth. Equation (8) calculates the energy used (in Joules, i.e., W) when a packet p is transmitted, while Equation (9) calculates the energy used when a packet p is received (size is represented in bits) [13, 19]

$$E_{TX} = V * I_{\text{Transmission Mode}} * (\text{Packet Size} / \text{Bandwidth}) \quad (8)$$

$$E_{RX} = V * I_{\text{Receiving Mode}} * (\text{Packet Size} / \text{Bandwidth}) \quad (9)$$

Since the energy spent on receiving and sending data packets and protocol packets are different, we need to evaluate the parameters in equations 8 and 9. Table 2 shows the NIC characteristics. In common conditions, the mode of a wireless card can be divided into four types, according to energy consumption, namely, doze, idle, receiving and transmitting. Except doze, we call the other three modes "active" state. In doze mode, neither sends nor receives signals; therefore, this is not suitable for MANETs.

For the most recent generation, 11 Mb/s data rates radio chip set, the values calculated remain similar. For example, the ORINOCO/IEEE Turbo 11 Mb PC card with the same power supply value (5V) has the following values: idle mode 15 mA; receive mode 240 mA; transmit mode 280mA. In GloMoSim simulator, wireless NIC is always in active state. NICs also consume energy when in the idle state, i.e., when simply powered on. However, in this work we assume that the idle status is energy free – as all the evaluated MANET protocols will have similar energy consumption, therefore, this can be ignored with little alteration in the results.

Now, utilizing the data from Table 2, we have $I_{\text{Transmission Mode}}$ = 330mA, $I_{\text{Receiving Mode}}$ = 280mA, V= 5V and Bandwidth =2Mbps. Again,

$$E_{Wh} = (Q_{mAh} * V)/1000 \quad (10)$$

Q_{mAh} is the charge in the battery. Equating equations 8, 9 & 10 we get the new modified equations, expressing charge in mAh unit (refer equations 11, 12).

$$Q_{TX} = 330 * \left(\frac{\text{Packet Size}}{2*10^6}\right) * \left(\frac{1}{3600}\right) \quad (11)$$

$$Q_{RX} = 280 * \left(\frac{\text{Packet Size}}{2*10^6}\right) * \left(\frac{1}{3600}\right) \quad (12)$$

Table 2. Modes of Wireless Card and Their Respective Current and Voltage used

Mode	Actual Current	Actual Voltage	Referenced Current	Referenced Voltage
Doze	14mA	4.74V	9mA	5V
Idle	178mA		Null	
Receiving	204mA		280mA	
Transmitting	280mA		330mA	

Since this charge is dependent on the packet sizes, we need to analyze the sizes of different protocol packets and data packets, with variable sizes. If we intend to have an efficient network, the packet sizes should be reduced compared to standard protocols. We have implemented this through our new set of packets, as explained earlier.

Table 3 has different packet lengths as mentioned, along with the total transmission and reception charge (in mAh) required by a node if all assumptions mentioned earlier, from Equations 8 through Equation 12, are satisfied.

As highlighted in Section 3, RREQ packet has a fail array section the size of which has an upper bound of (N-4), where N is the number of nodes, 10 in the test case. Since, a node can report fail for nodes other than itself, the next node, source node and destination node. We consider the data packet size to be 20 bytes. In the packet there are at most k sections, each 32 bits. Hence, we have 20*8 bits = 32 * k, hence k=5, i.e. there are 5 sections.

The total required threshold power for intermediate nodes is shown in Equation 13 and 14; and that for destination node, is shown in Equation 15 and 16.

$$\mu_i = NREP_{TX} + NREQ_{TX} + \left(\begin{matrix}NREP_{RX} + RREQ_{TX} + \\ Report_{RX} + Recco_{TX}\end{matrix}\right) * (n-i-2) + RREQ_{RX} + RREP_{RX} + RREP_{TX} + Data_{RX} + Data_{TX} + Ack_{RX} + Ack_{TX} \quad (13)$$

$$\mu_i\mu_i = 34.52*10\text{^-}6 * (n-i-2) + 80.65*10\text{^-}6 \text{ mAh} \quad (14)$$

$$\mu_d = RREP_{TX} + Data_{RX} + Ack_{TX} \quad (15)$$

$$\mu_d\mu_d = 30.02*10\text{^-}6 \text{ mAh} \quad (16)$$

Here, "i" is the message count, which is incremented for each node with each transmission of RREQ packet. At any time, a node can receive any number of NREPs, but will transmit and receive RREQ from only one reliable node, as decided by the fidelity judgment stage. The $NREP_{RX}$ is dependent on the number of neighbors. It is possible that an intermediate node might suffer several failures and has to resend RREQ to other remaining nodes in the neighbor table. Hence, $RREQ_{TX}$ is also dependent on the number of nodes. For the destination node, the node would only have to transmit a RREP, receive Data and transmit ACK packet to neighbor nodes. For each failed RREQ, a Report is received and a Recommendation is transmitted.

Table 3. Transmitting and Receiving Charge (in mAh) for Different Packets

Packet Names	Packet Size (in bits)	Transmission Charge TX (in mAh)	Receiving Charge RX (in mAh)
NREQ	64	2.93*10^-6	2.49*10^-6
NREP	96	4.40*10^-6	3.73*10^-6
RREQ	160+32(n-4) =352	16.13*10^-6	13.69*10^-6
RREP&REPORT&ACK	192	8.79*10^-6	7.47*10^-6
Recommendation	128	5.87*10^-6	4.98*10^-6
Data	160+32k=320	14.67*10^-6	12.44*10^-6

The number of neighbors for an intermediate node can be calculated by simply considering the message counts as the count increments with each RREQ hop. As defined earlier, message count, equivalent to number of hops, is given by i, and these nodes are not possible neighbor choices for transmission. A node also excludes itself and the selected neighbor for the number of possible neighbor choices. Therefore, the number of neighbor choices for a node is limited to a maximum of n-i-2, at any point of time, where n is the number of nodes in the network and 'i' is the message count.

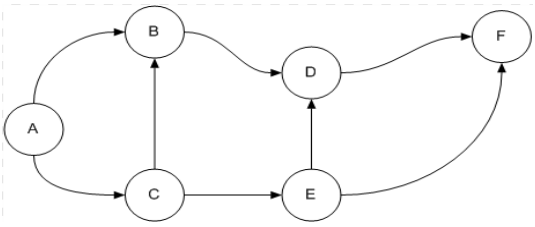


Fig.19. A simple 6 Node Network

Consider a simple example of a network, as shown in Fig. 19, with A as source, and F as destination. When node B sends its battery power in the NREP packet to node A, node A needs to know the number of neighbors of B (to which B can successfully transmit NREQ packets), in order to calculate the threshold battery power. For i=0 at node A, the maximum number of neighbor nodes possible for B is (n-2), i.e. all nodes except Node A and B. After the RREQ is sent to Node B, i=1 and node A is busy. So, node A will not reply to any packet except for a RREP from B. Next, D sends its battery value to node B, and B predicts the maximum number of neighbor nodes D can have; which is (n-1-2), since i=1, excluding both nodes B and D. Similarly, after sending the RREQ to node D, node B will be busy. Node D on receiving the destination F directly forwards the RREQ to F. Node F sends back the RREP with its own battery power, which is intern forwarded back to node A. At node A, the value of μ_d is checked. This makes node A certain that node D can receive the data and send back the acknowledgement packet easily.

The energy and battery constraints in this protocol adds a new dynamic that introduces extra amount of reliability to the network, so that the nodes can make an intelligent choice about the transmission and energy wastage is minimized. Since, this threshold calculation is dependent on the number of packets and its sizes, this method can be easily generalized and used by other systems.

VI. Security Analysis of IEFBOD

In this section we discuss the various strategies through which the malicious activities of the network nodes can be mitigated by IEFBOD protocol.

A. A Single Malicious Node on a Routing Path

- **Black hole attack:** A black hole [12] is any node which silently discards the data traffic without informing the source node. IEFBOD protocol bypasses the route containing the black hole, as it decrements the fidelity of a malicious node when it drops the data, and increments the fidelity of benign nodes, ensuring malicious nodes are never selected.
- **Gray hole attack**: A variation of black hole attack is the gray hole attack [11], in which the nodes will drop the packets selectively. In IEFBOD protocol, if a benign node starts acting maliciously, it will have its fidelity lowered; and if count = 3 (defined in Section 4), the node gets blacklisted, hence it is removed completely from the network. This is also explained in Section 4C.
- **Sybil attack:** Sybil attack [26] manifests itself by allowing malicious users obtaining multiple fake identities by pretending to be multiple, distinct nodes in the system. In IEFBOD protocol, fidelity parameter ensures that only trustworthy nodes are present in the network. Thus, Sybil attack is reduced to some extent.

B. Two or More Colluding Malicious Nodes Adjacent To Each Other

- **Cooperative Black hole**: In this attack a group of malicious nodes forwards the data packets amongst themselves thus, effectively exhausting the TTL of the packet and rendering it useless. IEFBOD prevents the same node to receive a message more than once due to the busy parameter and the

acknowledgment scheme; hence it can prevent this type of attack.

- **Wormhole attacks:** The wormhole attack [30] involves the cooperation between two attacking nodes, whereby the captured routing traffic at one point of the network is tunneled it to another point in the network. In IEFBOD protocol, the route request is sent to a node with the highest fidelity, moreover the route request packets are digitally signed, and when acknowledgement from source is not received within the timeout period, the wormhole route is avoided due to low fidelity.
- **Jellyfish Attack:** Jellyfish [1] affects packet end-to-end delay and the delay jitter but not packet delivery ratio or throughput. In this protocol, due to the delay caused, the acknowledgement received will be delayed and timer will expire, thus preventing this attack.
- **Blackmail attack:** In a blackmail attack [14], or more effectively a cooperative blackmail attack, malicious nodes complain against an honest node to make other nodes that need to send data to believe that routing through the victim is harmful. In IEFBOD protocol, three recommendations are required for blacklisting; moreover, the report packet registering the complaint needs to signed and if the signature is not verified the complaint is not registered against the node.

Apart from the above-mentioned attacks, IEFBOD with its fidelity and recommendation process can easily mitigate many other active and passive attacks.

VII. Simulation

A. Simulation Environment

Global Mobile Information System Simulator (GloMoSim) is a simulator environment which uses parallel discrete-event simulation based on Parsec [23]. For the purpose of our experiment, we consider nodes moving in a 500 meter * 500 meter region and we change the number of nodes from 30 to 100, with 20% malicious nodes. A space propagation model with a threshold cutoff is used as the channel model. We use the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. The mobility model is the random waypoint model, with minimal speed of 1 m/s, and the maximal speed of 10m/s. The pause time is 30s. We neglect over-hearing of peer-to-peer packets. The RTS/CTS option is turned off in the MAC layer. The 100-120 bits headers which will get appended by other layers have been neglected, since it will be same for all MANETs with same standards. We assume that the idle status is energy free as all the evaluated MANET protocols will have similar energy consumption. The total battery power is 1430 mAh. Data packet size is of 20 bytes with CBR type. Table 4 lists other simulation details.

Table 4. List of Simulation Parameters

PROPAGATION-LIMIT	-111.0
PROPAGATION-PATHLOSS	TWO-RAY
NOISE-FIG.	10.0
RADIO-TYPE	RADIO-ACCNOISE
RADIO-FREQUENCY	2.4e9 Hz
RADIO-BANDWIDTH	2000000 bits/sec
RADIO-RX-SNR-THRESHOLD	10.0
RADIO-TX-POWER	-10.0 dBm
RADIO-ANTENNA-GAIN	0.0 dB
RADIO-RX-SENSITIVITY	-91.0 dBm
RADIO-RX-THRESHOLD	-81.0 dBm
MAC-PROTOCOL	802.11

B. Simulation Output

In GloMoSim one can easily see the simulation in Java GUI, where the green line signifies the successful data transmission. Form Fig. 20, 21, 22, the successful transmission of data from node 3 to node 5, through nodes 7 and 6 can be easily observed. When there is a black hole/gray hole attack by node 6, packets are dropped, as shown in Fig. 21, signified by a red line. After this attack, the fidelity of node 6 is decreased and new node 2 is selected, hence the path is changed, as shown in Fig. 23.

Therefore, we can establish our claim that IEFBOD is able to handle standard attacks.

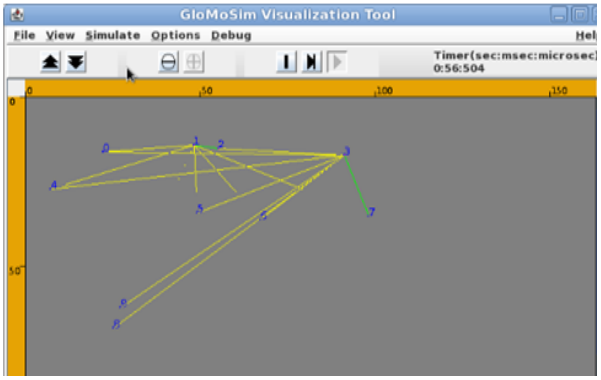


Fig.20. Data route (Node 3-Node 7)

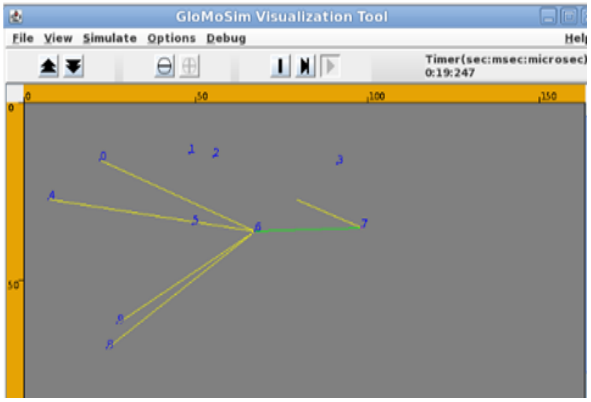


Fig.21. Data route (Node 7-Node 6)

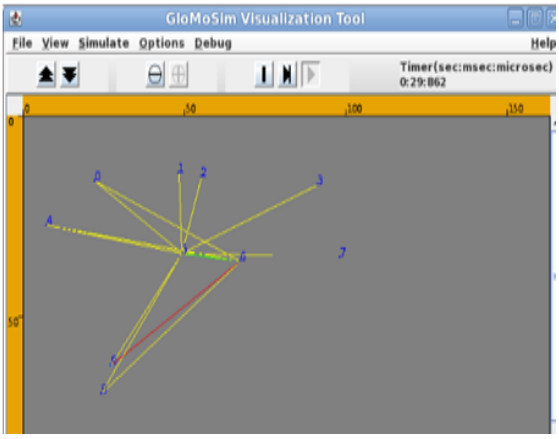


Fig.22. Data route (Node 6-5)

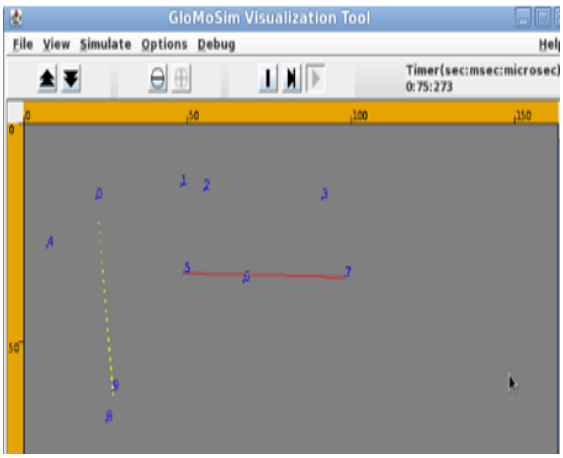


Fig.23. Attack by Node 6

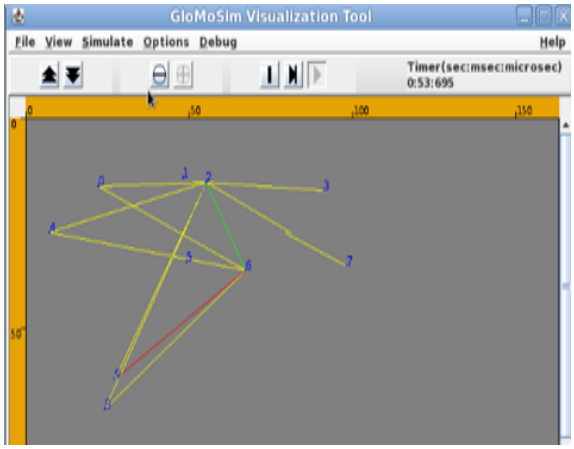


Fig.24. Change in Path via Node 2

VIII. Performance Analysis

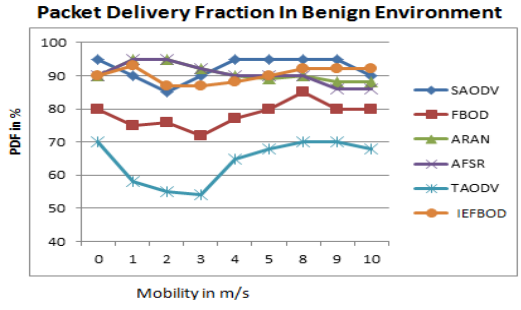
In this section we perform an analysis of our protocol on the basis of the performance metrics, and compare it with other popular secure routing protocols. Several QoS metrics can be used for performance analysis. We consider the packet delivery fraction (PDF), normalized routing load (NRL) and end-to-end delay, while varying mobility and number of nodes. We repeat the experiment in benign and malicious environments, and vary the number of malicious nodes. The sub-sections provide an overview of the methodologies, followed by the relevant graphs and analysis.

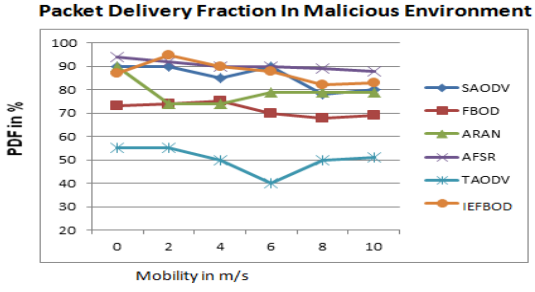
A. Overview of Methodology for Comparative Performance Analysis

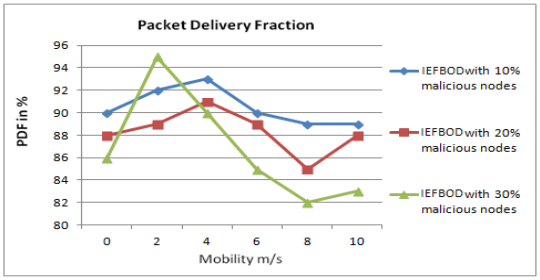
The test conditions mentioned in section 7A, have been used for performance evaluation of both our proposed secured routing protocol and other standard protocols i.e. ARAN, SAODV, TAODV, FBOD and AFSR. We have considered these protocols as they are well known and considered to be state of the art for on demand routing protocols. Therefore, our motivation is to establish that IEFBOD outperforms the current standard methods in several ways. PDF, NRL and end-to-end delay are standard parameters for comparison of accurate and robust routing in MANET, therefore, these are used for the simulations. The simulations also contain malicious nodes in order to obtain a comparative analysis of the security of the protocols. The mobility (in m/s) and number of nodes are the two variables considered to simulate the protocols and evaluate their performances. In order to correctly simulate the results and take accurate estimations, we run the simulations several times and take the average values of these results.

B. Analysis of Standard Secure Protocols

Traditionally, the shortest path to a destination (in terms of number of hops) is considered to be the best routing path. SAODV [2] explicitly seeks shortest paths using the hop count field in the route request/reply packets. ARAN, on the other hand, assumes that the first route discovery packet to reach the destination must have traveled along the best path. As discussed in Section 2, TAODV uses a trust concept and has extra packets, which make the protocol computationally heavy. IEFBOD on the other hand is an upgraded model of FBOD, which attempts to overcome problems such as battery issues that FBOD cannot handle.







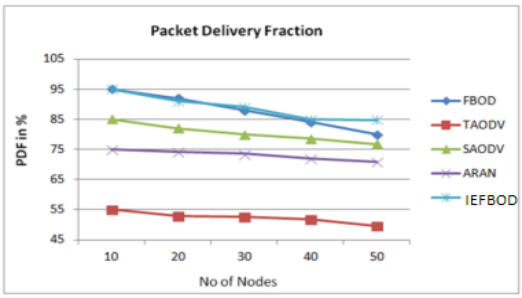
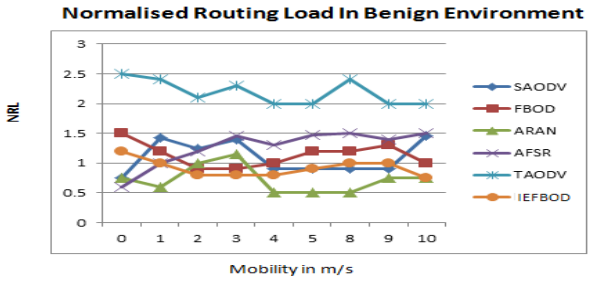
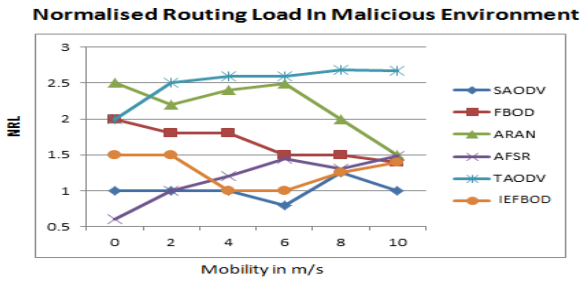
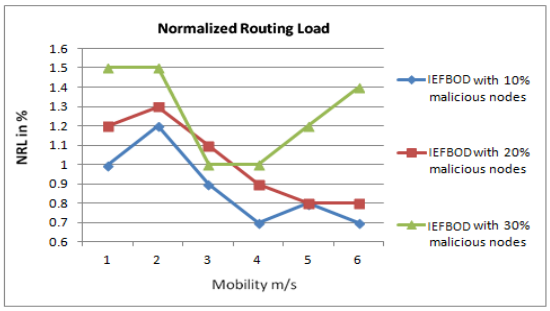


Fig.25. From top to bottom: (a) Packet delivery Fraction in Benign Environment (b) Packet delivery Fraction in Malicious Environment (c) Effect of Packet delivery Fraction in varying Malicious Environment, (d) Packet delivery Fraction with varied number of nodes

Each data point in Fig. 25-27, is an average of 10 simulation runs with identical configuration but different randomly generated mobility patterns.







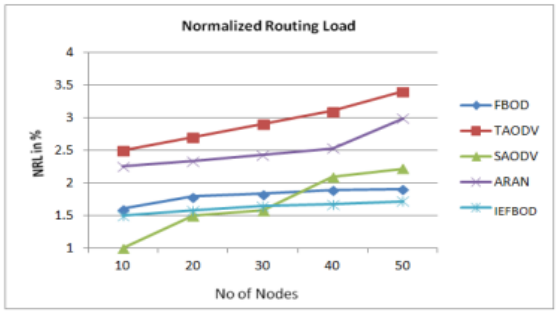
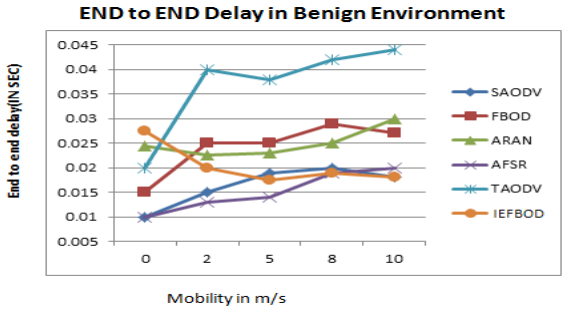


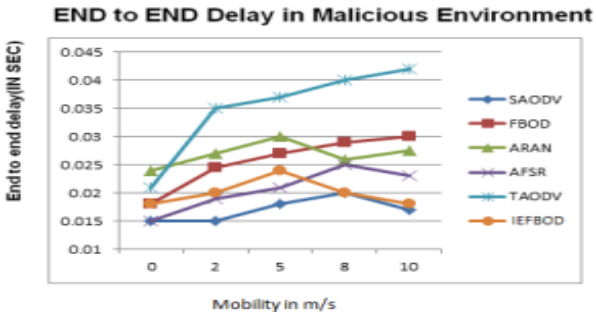
Fig.26. From top to bottom: (a) Normalized Routing Load in Benign Environment (b) Normalized Routing Load in Malicious Environment (c) Effect on Normalized Routing Load in varying Malicious Environment (d) Normalized Routing Load with varied number of nodes

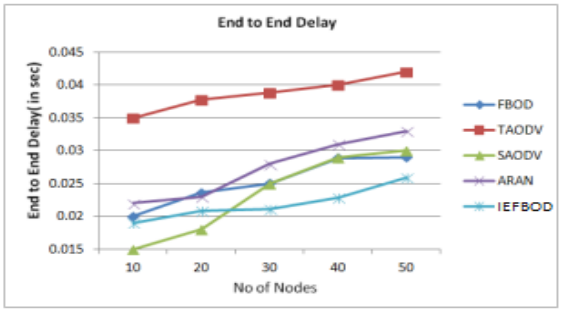
C. Analysis of Results from Simulation

1. Packet Delivery Fraction

From the graph in Fig. 25(a), it is observed that IEFBOD maintains competitive PDF when compared to other protocols in benign environments. As the malicious nodes are introduced into the environment our protocol slowly builds up the fidelity values, eventually blacklisting those nodes. These malicious nodes are eliminated from the network, hence preventing packet losses and unnecessary delays.







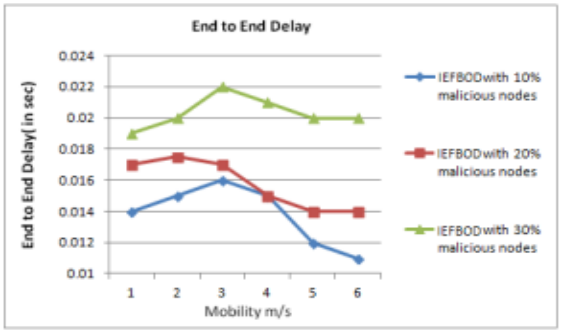


Fig.27. From top to bottom: (a) End to End Delay in Benign Environment (b) End to End Delay in Malicious Environment (c) Effect on End to End delay in varying Malicious Environment (d) End to End delay with varied number of nodes

IEFBOD shows on an average a PDF of 87%, as shown in Fig. 25(b), in malicious environments. Since our protocol selects the most reliable and secure path, the PDF is high. Fig. 25(d) shows the PDF with varying number of malicious nodes. At 30% malicious nodes and mobility 10 m/s, the PDF is 83%, highlighting that IEFBOD has high PDF in such scenarios. Fig. 25(c) shows PDF in an environment with 20% malicious nodes while varying the total number of nodes, where it is demonstrated that IEFBOD performs well even when the number of nodes is high.

Normalized routing load

The NRL for IEFBOD is on average 0.88 and 1.27 for benign environment and malicious environment, as shown in Fig. 26 (a) & Fig. 26 (b), respectively. After a certain point the malicious nodes are blacklisted and eliminated, hence leading to a stable and constant NRL. Since a lot of security measures would have to be taken, the routing load increases a lot in the case of ARAN, AFSR and TAODV. SAODV and FBOD are not able to eliminate the nodes from the network; the nodes have to route data in the presence of these malicious nodes, which leads to an unstable NRL. Therefore, IEFBOD outperforms these protocols in terms of stability and low value of NRL.

Fig. 26 (c) shows the NRL with varying number of malicious nodes. It is seen that the NRL lies between 1 and 1.5 even at 30% malicious nodes. Fig. 26 (d) shows the NRL in an environment with 20% malicious nodes while varying the number of nodes, where IEFBOD again demonstrates stable and low NRL.

2. End-to-end delay

Fig. 27 (a) shows the end to end delay for benign environment. The end to end delay initially is high, but slowly it reaches an average point and stabilizes. With time, the most secure route is discovered and hence the fluctuation in end-to-end delay is reduced significantly. Fig. 27 (b) shows the end to end delay lies between 0.018 to 0.025 seconds in malicious environment. This is significantly less compared to other secure routing protocols. Since we choose the most secure path, the probability of route failure or formation of routing loops is reduced for highly malicious networks. Fig. 27 (c) shows End to End delay with varying number of malicious nodes which is also only between 0.018 to 0.025. Fig. 27 (d) shows the end to end delay in an environment with 20% malicious nodes while varying the number of nodes, and IEFBOD clearly outperforms other protocols with increasing number of nodes.

3. Effect of Mobility in Performance Metrics

In the experiments, the network parameters are considered for different environments, while varying mobility in each case. For high mobility, the most significant impact is on PDF. This decreases to 83% for an environment with 30% malicious nodes and mobility of 10 m/s. Therefore, when mobility is high, some packets may be dropped by the protocol.

However, the protocol maintains stable and low NRL and end-to-end delay for high mobility. In fact, it outperforms the other protocols significantly, due to effective route selection and avoiding nodes with low battery power, which leads to delays in routing.

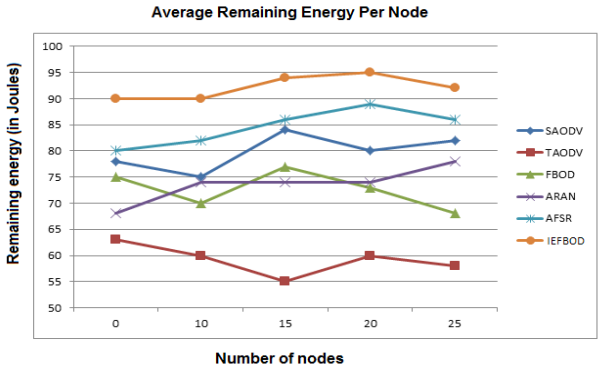


Fig.28. Average Remaining Energy versus Number of Nodes

D. Analysis of Energy Awareness and Efficiency

1. Energy Awareness

IEFBOD, being an intelligent energy aware protocol, has superior performance in case several nodes have low battery power. In such a case, while other protocols will select the nodes with low battery in the routing path, IEFBOD will not consider them. Moreover, the limits on battery prevent repeated selection of the same node which can occur in FBOD, AFSR etc. Therefore, IEFBOD performs better than other protocols in situations with several nodes having low battery levels. IEFBOD adds an additional decision of choosing optimal energy pathways while routing. Therefore, it dynamically responds to the current state of the nodes in the network. However, it uses a simple metric to ensure energy efficiency that can easily be implemented in other systems.

2. Energy Consumption

To demonstrate the effectiveness of the algorithm in terms of energy consumption, we use the same parameters and the energy equations computed in Section 5. The total energy for the nodes is 100J. Figure 28 shows the energy remaining on average for all the considered protocols. Clearly, IEFBOD has the highest average

energy left, with improvement of around 10-15% versus AFSR and over 20-30% over other protocols. The main advantage of the protocol is that it is unicasting and lightweight, which avoids unnecessary packet transmission.

E. Overall Comparison

From Fig 25 – 27, several observations can be made about the performance of IEFBOD in comparison to other trust-based routing schemes.

In terms of PDF, IEFBOD has similar packet delivery rates as other protocols in benign environments. For malicious environments, it outperforms all protocols except AFSR. For mobility between 0-5 m/s, the two protocols present similar results. However, for high mobility, AFSR has a minor improvement of around 8% at 10 m/s. This is a minor delta in performance, and on an average over all mobility values, IEFBOD has similar performance to AFSR.

For NRL, IEFBOD clearly outperforms other protocols like TAODV, FBOD, SAODV and ARAN either in terms of stability or with respect to low value of NRL. It distinguishes itself from AFSR by its performance at high mobility. While AFSR has low NRL for low mobility that increases with increasing mobility, for IEFBOD, the NRL starts out high, but stabilizes at a low value with high mobility. This establishes that mobility is not a significant issue in performance of this protocol.

In benign environment, IEFBOD has comparable end-to-end delay with the protocols it has been compared to. However, in malicious environments, especially at high mobility, IEFBOD significantly outperforms most protocols and is competitive with SAODV. In fact, AFSR has an end-to-end delay which is almost 35% more than that of IEFBOD for mobility 10 m/s and 30% malicious nodes.

Overall, in terms of the standard metrics, IEFBOD outperforms the standard protocols considered in this section. While the PDF for highly malicious networks is similar to that of SAODV and slightly less than AFSR, the protocol distinguishes itself by low end-to-end delay, stable NRL and ability to reduce energy consumption due to battery thresholds utilized for routing.

IX. Conclusions

IEFBOD has many unique features which make it more secure and reliable compared to other secure routing protocols as highlighted in Fig. 25-27 in Section 8. It is a unicast protocol, and it sends the RREQ packet to only one trustworthy node, based on the fidelity values. The use of busy flag prevents the cycling of RREQ packets. Moreover, the battery thresholds make sure that the nodes which are selected have enough battery power to send the data and control packets successfully. This selection of a secure and reliable node helps in detecting and mitigating wormhole and rushing attacks. The proposed protocol also performs well against attacks such as black hole, gray hole, blackmail and other attacks as highlighted in section 6. With each successful transmission, the fidelities of other non-malicious nodes increase, hence decreasing the chances of black hole node getting selected. Moreover, the recommendation and the count value monitor the eyehole and blackmail attacks quite efficiently. Nodes wait for a fixed and calculated time period for RREP and ACK packets to arrive, hence jellyfish attacks are reduced.

We have used new lightweight packets like NREQ and NREP, to update the neighbor table periodically. Performance of the protocol in other attacks can be assessed from Section 8. We can see from the performance metrics highlighted in Fig. 25-27 and Section 8 that our protocol works better in a malicious environment than other popular secure routing protocols, with high PDF, low NRL and average End-to-End delay. This is true while varying mobility as well as changing number of nodes.

Energy efficiency is implemented in this protocol using battery threshold calculations. These calculations are done dynamically prior to transmission of a message and ensure intelligent selection of the next hop in the algorithm. This leads to higher QoS parameters and, on average, lower energy consumption.

The aim of the protocol was to establish the usage of trust and energy parameters in a cooperative method. As highlighted in Section 8, the protocol outperforms the state of the art. Therefore, it effectively uses the novel idea of combining the two strategies for secure routing in MANET in a cohesive manner.

In the future we would like to implement the same protocol in hardware and implement a Personal Area Network, on Arduino Platform.

References

[1] A. Kaur and D. Singh (2013)"Effects of Jelly Fish Attackon Mobile Ad-Hoc Network's Routing Protocols" Int. Journal of Engineering Research and Applications, www.ijera.com, Vol. 3, Issue 5, pp.1694-1700.

[2] C. Perkins and E. Royer, (1999). Ad hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 1999), 80–100.

[3] C. Perkins and P. Bhagwat, (1994). Highly dynamic destination-sequenced distance- vector routing (dsdv) for mobile computers. In Proceedings of ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications, 234–244.

[4] D. Johnson and D. Maltz,(1996). Dynamic source routing in ad-hoc wireless networks routing protocols. In Mobile Computing. Kluwer Academic Publishers, 153–181.

[5] D.V. Park and M.S. Corson,(1997). A highly adaptive distributed routing algorithm for mobile wireless networks. In Proceedings of the 2nd IEEE INFOCOM, 405–1413.

[6] H.N Saha., D. Bhattacharyya, B. Banerjee, S. Mukherjee, R. Singh and Ghosh D.,(2014) Different Routing Protocols And Their Vulnerabilities And Their Measures. In Proceedings. of the International. Conference on Advances in Computer Science and Electronics Engineering CSEE, 192-202.

[7] H.N. Saha, D. Bhattacharyya, B. Banerjee, S. Mukherjee, R. Singh and Ghosh D.,(2013) A Review On Attacks And Secure Routing Protocols In Manet,in CIBTech,

International Journal of Innovative Research and Review (JIRR) Vol. 1, No. 2, 12-36.
[8] H.N. Saha, D. Bhattacharyya, B. Banerjee, S. Mukherjee, R. Singh and D. Ghosh,(2014). Self-Organized key management based on fidelity relationship list and dynamic path. International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 7.
[9] H.N. Saha, D. Bhattacharyya, P.K. Banerjee (2011). Fidelity Based On Demand Secure (FBOD) Routing in Mobile Adhoc Network,(IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Wireless & Mobile Networks.
[10] H.N. Saha, R. Singh, D. Bhattacharyya, (2015). Hardware Implementation of Fidelity based On Demand Routing Protocol in MANETs, IJCNIS, vol.7, no.8, pp.39-48, 2015.DOI: 10.5815/ijcnis.2015.08.05
[11] H.P Singh, V.P. Singh, R. Singh (2013), "Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review" IJCA Vol 64, No 3,pp.16-22.
[12] I. Ullah and S.U. Rahaman (2010).Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols. In Master Thesis Electrical Engineering Thesis no: MEE 10:62.pp.1-41.
[13] J.C Cano. and P. Manzoni,(2001). Evaluating the Energy-Consumption Reduction in a MANET by Dynamically Switching -Off Network Interfaces. In Proceedings of the Sixth IEEE Symposium on Computers and Communications (ISCC 2001), 3-5.
[14] K. Konate and A. Gaye (2011).A Proposal Mechanism Againstthe Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile AdHoc Network. International Journalof Future Generation Communication and Networking. Vol 4, Issue 2, pp.69-80.
[15] K. Sanzgiri., B. Dahill, B. Levine and E. Belding-Royer, (2002). A secure routing protocol for ad hoc networks. In Proceedings of 10th IEEE International Conference on Network Protocols (ICNP).
[16] L. Buttyan and J.P. Hubaux (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications 8(5) 579–592.
[17] L. Lamport, R.E. Shostak, and M. Pease (1982). The Byzantine Generals Problem.ACM Trans. Programming Languages and Systems, vol. 4, no. 3 pp.382-401.
[18] M. Abdelhaq, S. Serhan, R. Alsaqour and R. Hassan, (2011). A Local Intrusion Detection Routing Security over MANET Network. International Conference on Electrical Engineering and Informatics, Bandung, Indonesia.
[19] M. Tarique and R. Islam, (2007). Minimum Energy Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. In International Journal of Computer science and Network Security, Vol 7 No.11, 304-311.
[20] M. Zapata and N. Asokan (2002). Securing ad hoc routing protocols. In: Proceedings of the ACM Workshop on Wireless Security (WiSe'02).
[21] P. Johansson, T. Larsson., N. Hedman, & B. Mielczarek (1999). Routing Protocols for Mobile Ad-hoc Networks - A Comparative Performance Analysis. In Proceedings of the IEEE/ACM MOBICOM, 195–206.
[22] P. Papadimitratos and Z.J. Haas.,(2002). Secure Routing for Mobile Ad Hoc Networks. Mobile Computing and Communications Review 6(4).
[23] R. Bagrodia, R. Meyerr,(1997). PARSEC: A Parallel Simulation Environment for Complex System. UCLA technical report.
[24] R. Kalaivani and D. Ramya,(2013). Secure Protocol for Leader Election and Intrusion Detection in MANET. International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 3,62-66.
[25] R.K. Nekkanti and C.W. Lee (2004). Trust based adaptive on demand ad hoc routing protocol. In: Proceedings of the 42nd annual Southeast regional conference 88–93.
[26] S. Abbas, M. Merabti, D. Llewellyn-Jones, K Kifayat "Lightweight Sybil Attack Detection in MANETs "Systems Journal, IEEE Volume:7 , Issue: 2 June 2013. pp 236 – 248.
[27] S. Agrawal, S. Jain, S. Sharma (2011), "A survey of routing attacks and security measures in mobile ad-hoc networks", journal of computing, Vol 3, Issue 1, pp.41-48.
[28] S. Corson and J. Macker, (1999). Mobile ad-hoc networking (MANET): routing protocol performance issues and evaluation considerations, RFC 2501.
[29] V. Girdhar and G. Banga (2015), A Incentive Based Scheme to Detect Selfish Nodes in MANET, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, pp. 561-565.
[30] V. Mahajan, M. Natu, A. Sethi(2008). "Analysis of wormhole intrusion attacks in MANETS". In IEEE Military Communications Conference (MILCOM), pp. 1-7.
[31] Y. Hu, A. Perrig and D. Johnson, (2002). Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. In: Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02) 3–13.
[32] Z.J. Haas, M. R. Pearlman, P. Samar,(2002). The Zone Routing Protocol (ZRP) for Ad Hoc Networks. IETF Internet Draft.

Authors' Profiles

Himadri Nath Saha completed his Bachelor of Engineering from Jadavpur University, Kolkata and has received his Master of Engineering in Computer Science & Engineering from Indian Institute of Engineering, Science and Technology. He completed his Ph.D. in Engineering from Jadavpur University.

He is currently the Head of the Department of Electrical & Electronics Engineering in Institute of Engineering & Management, Kolkata. He has several publications in many international journals and conferences with many citations. He has also written a textbook on "Database Management System" which became popular among students. His research interest includes machine learning, IoT, wireless communication, Mobile Ad-hoc Networks, network security, cryptography and algorithms.

Dr Saha is associated with different professional bodies like IEEE, ACM and IEI. In the year 2013, he has received Gold Faculty Award from Infosys Technology Limited. In the year 2012, he was also given the "Best Faculty Award" for presenting an innovative case study, among several professors from reputed universities by Infosys Technology Limited. Dr. Saha has also received many more awards in the fields of education and research in the last decade.

Prachatos Mitra is a student in Institute of Engineering and Management. He is currently studying for B.Tech in Computer Science and Engineering, and will be graduating in 2018.

How to cite this paper: Himadri N. Saha, Prachatos Mitra,"Intelligent Energy Aware Fidelity Based On-Demand Secure Routing Protocol for MANET", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.4, pp.48-64, 2018.DOI: 10.5815/ijcnis.2018.04.06