IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Mitigating Randomized Selfish Behavior Attack Using Trust-Confidence Aware OLSR for Efficient Data Communications

K. A. Adoni[1*], A. S. Tavildar[2], K.K. Warhade[3]

[1] Dept. of Electronics and Telecommunication, VIIT Research Centre, VIIT, Savitribai Phule Pune University, Pune, India
[2] Dept. of Electronics and Telecommunication, VIIT College of Engineering, Savitribai Phule Pune University, Pune, India
[3] Dept. of Electronics and Telecommunication, MIT College of Engineering, WPU University, Pune, India

[*]*Corresponding Author: akirti2008@gmail.com, Tel.: +91-98505-43828*

Available online at: www.ijcseonline.org

Accepted: 20/July/2018, Published: 31/July/2018

***Abstract*—** Data communication performance of Mobile Ad-hoc Networks (MANETs) gets adversely affected by presence of malicious nodes. In this paper, model for random On/Off switching, referred as selfish or malicious nodes has been used, with OLSR protocol and a simple trust strategy has been proposed to decide the trust of next hop node. Residual energy level of forwarding node is also continuously monitored and accordingly confidence level associated with the node has been determined. Continuously varying trust parameter and confidence levels of all forwarding nodes have been incorporated in the Hello and Topology Control (TC) message formats of standard OLSR protocol. Further, OLSR protocol has been modified using Trust and Confidence values of nodes. The proposed protocol, termed as OLSRT-C, has been used to select the optimum path for data forwarding. Simulations carried out on typical MANET scenario show that the proposed OLSRT-C protocol successfully mitigates randomized Selfish Behavior (SB) attack significantly with marginal increase in the Average Energy Consumption per node.

***Keywords*—**MANETs, Selfish Behavior attack, OLSR, Trust-Confidence routing, PDR, Routing Overheads, Average Energy Consumption

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) consist of self-configuring networks without any central fixed infrastructure. The nodes are connected via point to point radio links and form its own ad-hoc network topology. Each node can act as a source, routing or destination node. The distance between source node and destination node decide the number of hop/s required for communication. Each node is mobile in nature; it is free to move anywhere in the network area. If the node moves in some other direction or out of the network, it will not be available for the routing purposes. This leads to frequent changes in links/routes resulting in dynamic network topology. Effective delivery of data packets with minimum routing overheads becomes vitally important factor in MANETs. In case of proactive routing protocols, Optimised Link State Routing protocol (OLSR) [1] has been often preferred in MANETs. In OLSR protocol, the routing overheads get reduced with Multi Point Relay (MPR) mechanism.

It is assumed that all nodes in MANETs are trustworthy and co-operative, i.e., all nodes perform in accordance with the self-defined specifications of the protocols [2]. Most protocols like Destination-Sequenced Distance-Vector Routing (DSDV) [3], Ad-hoc On demand Distance Vector (AODV) [4], Dynamic Source Routing (DSR) [5], OLSR [1] etc. adhere to this philosophy. However, this hypothesis is often violated due to the nodes' restricted resources like battery power, memory etc. Further the MANETs are vulnerable to various types of attacks. The performance of MANET degrades due to various attacks, like Black Hole, Selfish Behavior, Denial of Service (DoS), Wormhole etc. [6]. In order to save their resources, nodes behave selfishly and deny taking part in forwarding packets of other nodes. The node switches to 'OFF' state for some time interval and makes itself unavailable for packet forwarding. Such type of attack is called as Selfish Behavior (SB). To prevent its detection of selfish behavior, node switches between 'ON' to 'OFF' states randomly. Randomized model has been proposed for SB attack [7], and to further compliment it with possible selfish behavior due to depleting energy resources of nodes a concept of confidence level of nodes has been proposed here. Basic OLSR protocol has been used by incorporating trust-confidence values of nodes. The MANET performance has been simulated using NS-2 simulations, by varying levels of maliciousness. While simulating network

performance, random node placement with random movement of nodes has been used. Further random ON/OFF switching of malicious nodes used as per the model [7] has also been considered in NS-2 simulations.

I.I. Specefic Contributions of the paper

The previously developed Basic random model for SB attack [7] has been complimented with energy depletion based selfish behavior. Appropriate Trust and Confidence based routing strategy has been proposed. MANET performance has been simulated for both, normal OLSR and modified OLSR termed as OLSRT-C protocol. The results indicate that with the use of OLSRT-C strategy, the degradations due to presence of SB attacked malicious nodes get significantly reduced, with much reduced degradations in routing overheads.

The rest of the paper is organized as follows. Related work in this topic has been briefly reviewed in Section II. The proposed routing framework has been explained in Section III. Section IV includes simulation scenario. Section V includes the results and discussion on MANET's performance, followed by Section VI, which concludes the paper.

II. RELATED WORK

Different types of malicious attacks have been observed [6, 8, 9, 10, 11, 12, 13 and 14] in MANET. Either mathematical or statistical models [15, 16, 17 and 18] have been investigated for MANETs. Extensive research investigations have been carried out in the area of detecting the malicious presence through various schemes, such as Watchdog managers, Malicious Node Detection Scheme (MNDS), Intrusion Detection, various methods of assigning positive/negative scores, voting, credits/penalties etc. The focus of this paper is on performance evaluation of MANET, degraded by selfish behavior attack. Thus, only those papers dealing with trust-confidence based routing and also involving MANET performance assessment, have been considered for review in the following paragraphs.

Rajaram et al. [6] have discussed various types of attacks, which can affect the network's performance. Trust based security protocol based on a MAC-layer approach has been developed. Trust values have been used to favor packet forwarding by maintaining trust counter for each node. Reward or punishment has been given based on node's behavior. If the trust value falls below predefined threshold, the node has been declared as malicious. The simulations show that packet delivery ratio (PDR) has increased from 60% to 80%. The slight decrease in delay has been observed. The routing overhead packets have also decreased considerably with rise in number of attacker nodes and also with the mobility of nodes. Odedra et al. [19] have discussed monitoring, isolation and detection of selfish nodes using Watchdog Method. Based on the time taken for packet forwarding, the nodes have been considered as selfish or normal. The network performance has been evaluated using AODV protocol. With the network of 25 nodes, the numbers of selfish nodes have been increased from 2, 4, 6 and 8. It has been observed that PDR has increased by 1.7 times, for modified AODV, compared to normal AODV. However, authors have also considered network size of nodes with 25, 50, 75 and 100 with only one node assumed to be malicious. They have reported that with modified AODV protocol, PDR has been improved by 1.8 times for network size of 25 nodes and 100 nodes. However, the PDR has improved only by 1.2 times for network size of 75 nodes and around 1.1 times for network size of 50 nodes. Roy et al. [20] have discussed probabilistic evaluation model using Beta probability density function along with node's energy. Energy factor has been used to calculate aggregate trust. AODV protocol has been used during simulations. The simulation results indicate that packet delivery ratio has improved marginally. Gong et al. [21] have proposed trust model based on neighboring node's behavior. DSR protocol and its modified trust version have been used for simulation. By considering percentage of malicious presence up to 50% of total nodes, packet delivery ratio has improved by 20%. Soni et al. [22] have proposed IDS scheme, which shows considerable improvement against selfish behavior attack. The malicious nodes absorb all the packets through faulty route reply (RREP) message; hence the senders were unable to obtain the ACK message from the receiver. This has resulted in drop of almost all the packets. After applying IDS, network performance, for packet delivery ratio has been enhanced from 15% to 92%. For simulation AODV protocol has been used. However, only 'one' node has been considered as selfish node in the network of 30 nodes.

Kirubakaran et al. [23] have proposed the simple Enhanced Triple Umpiring System (ETUS) for packet forwarding procedure to deal with different attacks. Network performance has been simulated with the use of AODV and modified AODV protocols for 30% of malicious nodes. It has been observed that the packet delivery ratio has increased marginally with considerable increase in routing overheads for modified AODV routing protocol. Singh et al. [24] have discussed Token Based Umpiring Technique (TBUT). Every node needs a token to participate in the network and neighboring nodes act as an umpire. If the nodes drop the packets, umpire sends an error message. TBUT has been compared with ETUS. With 30% of malicious nodes in the network, marginal improvement has been observed with respect to ETUS. Kampitaki et al. [25] have defined selfishness based on energy level of nodes. Based on residual energy levels, different levels of selfishness have been defined. Increasing selfishness affects the network's

parameter i.e. packet delivery ratio adversely. Geetha et al. [15] have discussed trust model based on node's trust and hop count. These parameters have been calculated using Bayesian Statistical Method. Either incentives or penalties have been assigned to nodes based on their capability to forward the packets successfully within the stipulated time. Network performance has been compared with AOMDV and trust based TBAOMDV for packet delivery ratio, overheads and end-to-end delay. For TBAOMDV, by varying, threshold value for trust, PDR has been increased remarkably with only marginal increase in routing overheads and end-to-end delay.

Banerjee et al. [26] have considered reputation based Trust Management System (TMS) for MANETs. The network performance has been evaluated using AODV protocol. It has been reported that with 20% maliciousness, the packet delivery ratio and throughput performance have been improved by around 25-30%, by using TMS based modified routing protocol. However, it is expected that it would also increase routing overhead considerably, as separate vector has been proposed and each node has to maintain and update all trust vectors. Venkatraman et al. [27] have presented regression based trust model for MANET, which includes trust vector model based on multiple parameters, like participation in routing, data forwarding, transferring the data without modification etc. The routing protocol has been modified by addition of trust-confidence values. Network evaluation has been carried out using both, AODV and OLSR protocols. Results reported for the OLSR protocol with 20% malicious nodes, indicate that throughput using Trust based OLSR protocol increases approximately by 4.5 times, compared to throughput with the normal OLSR protocol. The end-to-end delay has also marginally increased for OLSR with VAR trust. However, it can be readily seen that routing traffic has increased nearly by 25% compared to normal OLSR. This can be expected because of exhaustive trust modeling assumed by the researchers.

Based on the above, it can be seen that many researchers have evaluated MANET's performance in presence of malicious nodes. Some have used trust based routing strategies to improve the network's performance. It has been observed Malicious level considered is limited (some of the researchers have assumed only one malicious node in network size of 30-75 nodes). However, most of the investigations have been based on the use of on-demand routing protocol, in which routing overheads of modified protocol increase significantly. OLSR protocol, which essentially is a proactive routing protocol, has been proposed to minimize the routing overheads. Very few researchers have investigated attack mitigation using OLSR protocol. Venkatraman et al. [27] have considered elaborate VAR trust model with about 20% maliciousness and have used both AODV and OLSR protocols. Even though considerable improvement in throughput performance has been reported, the routing traffic volume, even with OLSR protocol, appears to have gone up by 25%. This increase in routing overheads can be controlled by appropriately deciding the trust-confidence assignment strategies, in order to significantly reduce the packet losses due to malicious presence.

III. PROPOSED ROUTING FRAMEWORK

A. *Attack Modelling and Mathematical Background*

The delivery of data packets gets adversely affected due to the presence of malicious nodes and the performance of MANET degrades due to various attacks, like Black-Hole, Selfish Behavior, Denial of Service (DoS), Wormhole etc. [6]. This paper focuses on Random Switching ON-OFF of malicious nodes or Random Selfish Behavior (SB) attack. In this attack, to prevent the malicious detection, the node changes its states randomly.

Different ways in which selfish attack can occur could be as follows:

1. Nodes take part in route creation, but refuse to forward packets of other nodes.
2. Nodes neither participate in the route creation phase, nor forward the data packets of others. They use their own resources for forwarding their own packets only.
3. Nodes change their ON/OFF status randomly, depending on their energy level. Initially when the energy is full, they behave properly like normal node. However, as the energy depletes, they start misbehaving. To preserve their own resources, the nodes switch between 'ON' and 'OFF' states for different time intervals.

This paper not only focuses on the last type of SB attack due to random 'ON/OFF' switching of nodes, but also on the selfish behavior of nodes due to energy depletion.

For example j^{th} node in the network is suspicious and considered to be selfish, then its ON-OFF behavior can be visualized as in figure 1 [7].

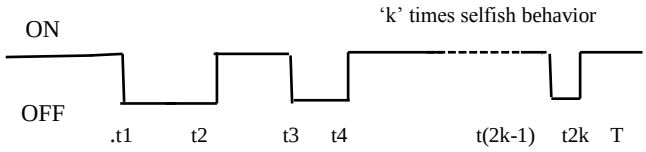


Figure 1. Illustration of typical Selfish Behavior of malicious node due to random On/Off switching

Service is 1blocked during the time interval 'Ƭ', when the nodes are in "OFF" state and the node switches to 'OFF' state 'k' times [7].

$$\tau = \tau_1 + \tau_2 \cdots\cdots + \tau_k = \sum_{i=1}^{k} \tau_k \quad (1)$$

When node switches ON/OFF, 'k' times, where 'τ_k' can be expressed as:

$$\tau_k = \sum_{k=1}^{k} (t_{(2k)} - t_{((2k)-1)}) \quad (2)$$

Theoretically, SB attack can be either deterministic [28] or totally random. In actual practical situations, any attack cannot be purely deterministic. The Selfish Behavior of nodes may always be random in nature and the randomness can be due to:

1. 'n' - Randomness in number of nodes, which behave selfishly.
2. 'k' - Number of times a given selfish node switches from 'ON' to 'OFF' and 'OFF' to 'ON' states.
3. 't_i' - Precise time at which the malicious nodes switch the state.

The following assumptions have been made in the proposed model [7]:

1. Number of malicious nodes 'n' in the MANET, n < N, have been considered as discrete random variables, where 'N' represents the total number of nodes in the network.
2. Number of ON/OFF pulses 'k' for given malicious node has also been viewed as discrete random variable.
3. All t_1, t_2……$t_{(2.k)}$ have been considered as continuous random variables, between 0 to T, where T is the total observation time.

Further in the proposed model, it has been assumed that the discrete random variable 'n' are Binomially distributed, 'k' number of times the given malicious node switches to 'OFF' state, during the total observation time 'T' has been assumed as, either Uniform or Poisson distributed. In this paper, the probability distribution of 'k' has been assumed as Poisson distribution. The absolute time instances 't_i' (1 < i < (2.k)), at which the malicious node changes the state, have been assumed as conditional uniform distribution in the available time i.e. probability density function (pdf) of 't_i' can be expressed as [7]:

$$f(t_i / t_{(i-1)}) = \frac{1}{(T - t_{(i-1)})} \quad (3)$$

Here, it has been assumed that different random variables i.e. 'n', 'k' and various 't_i' are all statistically independent random variables, where 1 < i < 2k and 't_0' has been either considered as zero, or starting time of network operation.

The probability of blocking due to j^{th} node has been expressed as [7]:

$$P_{bj} = \frac{1}{T} E(\sum_{i=1}^{k} \tau_i / k).P_k \quad (4)$$

In this equation, the symbol 'E' represents statistical averaging operation and P_k as probability density function of random variable 'k', assumed to be Poisson distributed [7] in the analysis.

$$P_k = \frac{(\lambda t)^k}{k!} e^{(-\lambda t)}$$

The total network blocking probability, P_B due to various selfish nodes in the MANET has been expressed as [7]:

$$P_B = \frac{E(n)}{N.T} \int_0^T \int_{t_1}^T \cdots \int_{t_{(2k-1)}}^T (t_2 - t_1 + \cdots + t_{2k} - t_{(2k-1)}) \frac{1}{\prod_{i=1}^{(2k-1)} (T - t_i)} dt_{(2k)}.dt_1 P_k \quad (5)$$

Symbol '$\prod$' represents multiplication.

In the mathematical modelling paper [7], the above blocking probabilities for individual selfish node P_{bj} and total network blocking probability P_B have been estimated, and different curves have been plotted. These results have been further used in this paper to decide the trust assignment strategy for Trust-Confidence Aware Routing Protocol, called 'OLSRT-C', proposed in this paper.

B. *Proposed Routing Strategy*

1) Normal OLSR Routing Strategy:

The process of routing in OLSR [1] depends upon periodical transmission of control packets. OLSR reduces the amount of control packets diffusion in the network with the help of Multipoint Relay (MPR) nodes. Two type of control messages are used - Hello and Topology Control (TC) message. The Hello and TC messages give information about one hop and two hop neighbors respectively. The formats of these messages are as shown in figure 2(a) and 2(b).

Individual nodes use the information of Routing Table and Topology Table to compute the path to destinations using 'shortest hop' scheme.

The limitations of shortest hop/ single path routing scheme have been:

1. Congestion in the network
2. Considerably increased energy depletion of some nodes located on shortest route.

These limitations lead to the increased packet loss probability, if some of the nodes on the path behave selfishly.

Reserved		Htime	Willingness
Link Code	Reserved	Link Message Size	
Neighbor Interface Address			
Neighbor Interface Address			
…..			
Link Code	Reserved	Link Message Size	
Neighbor Interface Address			
Neighbor Interface Address			

Figure 2(a): Hello message format

ANSN	**Reserved**
Advertised Neighbor Main Address	
Advertised Neighbor Main Address	
…..	

Figure 2(b): TC message format

2) Trust-Confidence Aware OLSR (OLSRT-C) Routing framework:

To avoid limitations of single shortest path, OLSR has been modified to multiple paths (multipath) OLSR [29]. It is presumed that nodes participating in MANET behave co-operatively obeying the routing protocol, which is used for communication. However, this is seldom the case and the mobile nodes in the MANET are vulnerable to various types of attacks. To avoid above mentioned selfish behavior attack, a trust-confidence aware protocol, OLSRT-C, has been proposed here. As OLSR has been based on proactive routing, the up-to-date routing table is being maintained with the help of Hello and Topology Control (TC) messages. At regular intervals, emission of Hello and TC messages take place to find out the information about the link status [whether symmetric, asymmetric or link lost] between the nodes. Based on this assignment, the trust levels has been decided. Each node maintains a routing table to all known destinations in the network. The 'reserved' field in the Hello and TC message format has been used to convey the trust and energy levels.

3) Trust and Confidence level assignment procedure:

Initially, the trust of all the nodes has been set to 'one', assuming that all nodes to be fully charged and therefore, behaves co-operatively to start with. The source routing method which consists of the Hello message, has been used to get multiple and trustworthy paths. The validity time and symmetric link have been used to determine the trustworthiness of the next forwarding node. The transfer of data can occur, if and only if, the link between two neighboring nodes has been symmetric. The link sensing helps each node to learn the knowledge of its neighbors, up to two hops. If the data gets received by the next one hop node within the specific time interval, designated as validity time (VT) interval, the next node has been considered to be trustworthy. The next node then checks for its next one hop neighboring node and the process continues till the destination. If the link between the neighboring nodes has been symmetric and data transfer takes place successfully within the VT interval, then trust level has been retained as 'one' for the next one hop neighboring node.

However, some of the nodes in the network may behave selfishly. If any of the node switch to 'OFF' state from 'ON' state, the link will become asymmetric or will be lost due to link breakage. Data transfer cannot take place from that node during that interval. This indicates that the node has been behaving selfishly. The link status has been continuously monitored between the node and its next one hop node. If the link has been asymmetric, then the next node is considered as a selfish node. The trust of that selfish node has been reduced by small factor 'Δ', (Δ<1). Therefore, the new assigned trust becomes (1-Δ). If the same node switches from 'OFF' to 'ON', provided the link becomes symmetric, the assignment of trust has been unaltered and retained as (1-Δ). If the malicious node switches from 'ON' to 'OFF' and again 'OFF' to 'ON', k=1 has been considered.

Further, if the same node again switches from 'ON' to 'OFF', link breakage has taken place again within the next VT interval. Then, the trust of that node has been further reduced by factor 'Δ', and the new trust value of that node becomes (1-(2.Δ)).

Now even if that node switches from 'OFF' to 'ON', the assigned trust has been retained unchanged to (1-(2.Δ)). From the analysis in modelling paper [7], it has been observed that probability of blocking is more for k⩾2. If the malicious node further switches from 'ON' to 'OFF' and 'OFF' to 'ON' i.e. k=3, then the assignment of trust has been reduced to (1-(3.Δ)), which has been considered as totally uncooperative node and its trust value should be approximately zero.

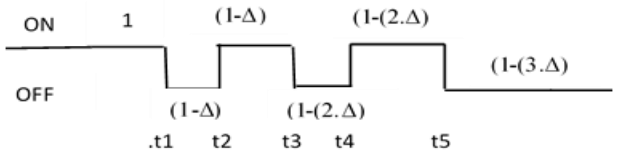


Figure 3: Proposed trust assignment strategy

Therefore, the small fraction 'Δ' has been taken as 0.33. The trust assignment strategy totally depends upon 'k'- number of times the malicious nodes switches from 'ON' to 'OFF' and again to 'ON' state. The proposed trust assignment strategy has been depicted in figure 3.

In addition to random ON-OFF switching, nodes may be depleting their energy resources and the malicious nodes may behave selfishly to preserve their energy. For this, residual energy 'E_R' of the node has also been continuously monitored. Energy tag 'E_{ti}' of the selfish node 'i' has set either to +1 or -1 as per the following rule.

$$E_{ti} = +1, if\ E_R/E_0 \rangle 0.3$$
$$E_{ti} = -1, if\ E_R/E_0 \leq 0.3 \quad (6)$$

In this equation, where 'E_0' is the initial energy of the node, has been considered as 10 Joules for simulation purpose, and 'E_R' is residual energy of the node at the given instant. As explained above, the nodes start misbehaving depending on their energy level. Further, it has been observed that in general the mobile nodes operate satisfactorily up to residual energy level of 2.5 to 3 Joules. Considering this minimum required residual energy level, it can be seen that an E_R/E_0 ratio of 0.3 has been considered as a threshold. Based on this factor of E_R/E_0 equal to 0.3 has been assumed in equation (6), to determine discrete energy tags 'Eti' for any malicious node 'i'.

The continuously varying trust value 'Ti' and energy tag 'E_{ti}' of nodes have been incorporated in 'reserved' field of standard Hello and TC message formats of OLSR protocol. Thus, it would help to avoid additional control bits in OLSR protocol, which will help to reduce the overheads further. When Hello and TC messages get exchanged, the updated trust and energy tag information for the nodes gets updated to all nodes, including the source nodes in the network.

4) Determination of Average confidence value of path:

There could be multiple paths available between given source-destination pair. Once the trust values and energy tags of all the nodes in the network have been assigned (by their immediate preceding nodes), confidence level 'Ci' of the node has been determined using following equation.

$$C_i = +1, if E_{ti} = +1 and T_i \geq (1-(2\Delta))$$
$$C_i = -1, if T_i \langle (1-(2\Delta)) or E_{ti} = -1 \quad (7)$$

Now, using trust 'Ti' and confidence level 'Ci', the average confidence value of given path has been determined by:

Average Confidence value of path =

$$\sum_{i=1}^{N_P} (T_i.C_i)/(N_P - 1) \quad (8)$$

In the above equation, 'Np' represents total number of nodes from source to destination in the given path. The modified OLSRT-C protocol selects the path with maximum average confidence value, as the preferred path for data transmission.

IV. SIMULATION SCENARIO

Simulations have been carried out using Network Simulator NS-2.35. Simulation parameters used for simulations have been summarized in Table 1. The step-by-step simulation sequence has been depicted in figure 4.

Taking into consideration the typical sizes of educational campuses in and around Pune city, such as Vishwakarma Educational Campus at Kondhwa, Pune-48, the typical network size of 1000mx400m has been assumed in this paper.

One can consider other possible network sizes of small 500mx500m, medium 1000mx1000m or large 5000mx5000m. For small network sizes the deployment of nodes could be dense, whereas for large network sizes the deployment of nodes could be sparse. The simulation time has been considered as 100 seconds, as it is a fairly long time to transfer large amount of data with the data rate of 20kbps. Further, the increase in Simulation Time would only lead to increase in computation time. Every reading has been noted, considering the average of four possible random scenarios –

1. 10 random iterations for mobile nodes placement (seed S1)
2. 10 random iterations for distribution of number of selfish nodes (seed S2)
3. 10 random iterations of, number of On/Off switches 'k' (seed S3)
4. 22 iterations for different random samples for time settings of absolute time 'ti' of malicious nodes (seed S4)

Each reading has thus been taken considering average of 10x10x10x22 i.e. 22,000 iterations of simulation readings, indicating that average of all random possibilities have been incorporated in the averaged results.

Table 1 Simulation Parameters

PARAMETER	SETTINGS
Network Area	1000m x 400m
Number of Nodes	40
Simulation Time	100 sec
Pause Time	0 sec
Speed of Nodes	0 – 5 m/s
Traffic Type	CBR
Radio Range of a node	250 Meters
Mobility Model	Random way point [30]
Packet Size	512 bytes
% of Malicious Nodes	10%-50% : steps of 10
'k' no. of On/Off Switching	Poisson distribution
Maliciousness- Mean k - m_k	Low=1, Medium=2

This process has been repeated by varying the percentage of selfish nodes from 10%, 20% up to 50% of nodes assumed as selfish in the network. Further, two levels of maliciousness, low level and medium level as proposed in [7] have been considered for performance evaluation. The simulation presumes that number of selfish nodes 'n' as binomially distributed and 'k' number of ON-OFF switching of selfish nodes to be Poisson distributed. The results of simulation have been presented in the following section.

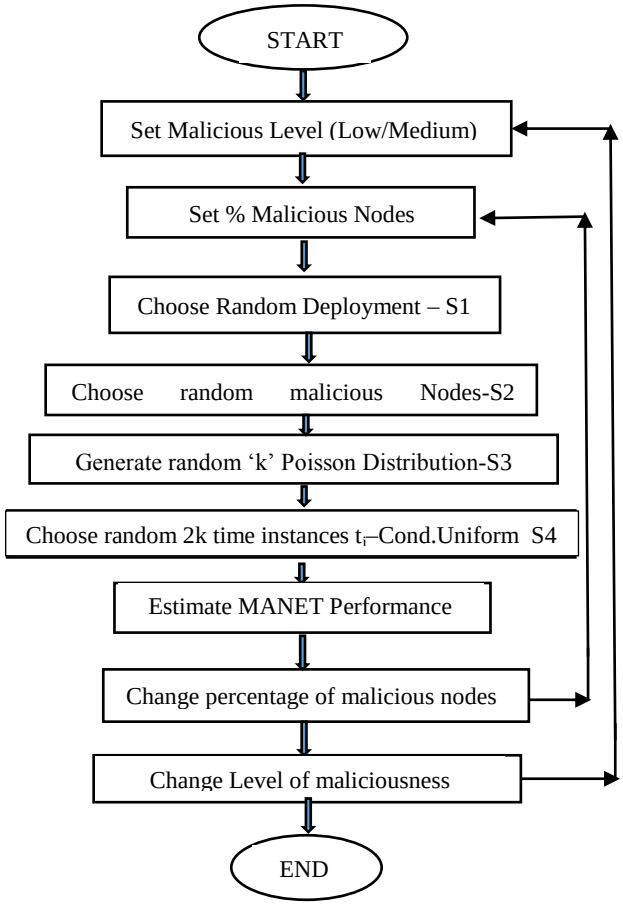


Figure 4: Simulations sequence considered

V. RESULTS

Three performance parameters namely Packet Delivery Ratio (PDR), Routing Overheads and Average Energy Consumption per node of the network have been used to compare the performance of OLSRT-C protocol with normal OLSR protocol.

A. *Definition of Performance Parameters:*

a) Packet Delivery Ratio (PDR):

It is the ratio of total number of packets received by the destination nodes to the total number of packets sent by source nodes. PDR has been expressed in percentage (%) value.

b) Routing Overheads (RO):

It is the ratio of total number of routing packets used in the path to the total number of data packets received by the destination [28]. This represents Routing Overheads in absolute number of routing packets that are used by the network per data packets successfully transmitted by the network.

c) Average Energy Consumption (AEC):

Due to the limitation of the battery resources in mobile ad hoc networks, monitoring of consumption of energy by each of the nodes in the network has been carried out. The average energy consumption found to be more for multipath type protocols compared to single and the shortest path type protocols. Average Energy Consumption per node of the network has been determined using-

$$AEC = \sum_{i=1}^{N} \frac{(E_0 - E_{Ri})}{N} \quad (9)$$

In this equation, 'E_{Ri}' represents residual energy of 'i^{th}' node at the end of the network simulations.

Figure 5 and figure 6 graphically show the simulated network performance for the three parameters PDR, RO and AEC, for low level maliciousness i.e. m_k =1 and for medium level maliciousness i.e. m_k=2 respectively.

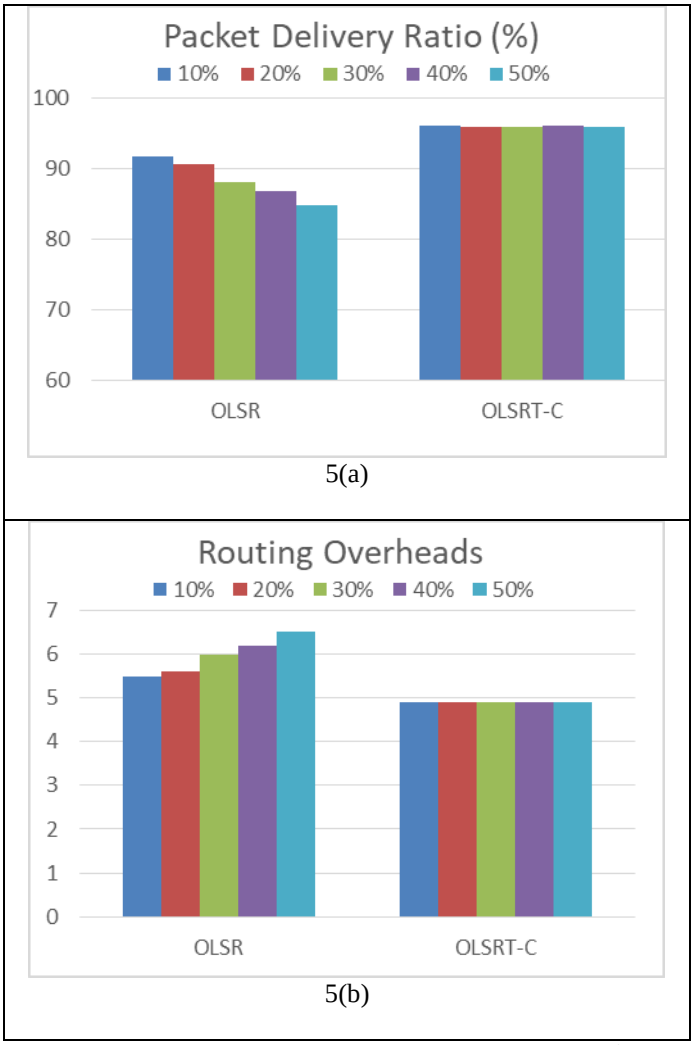


Figure 5 (a) and (b): Packet Delivery Ratio and Routing Overheads for low level maliciousness, i.e. m_k=1

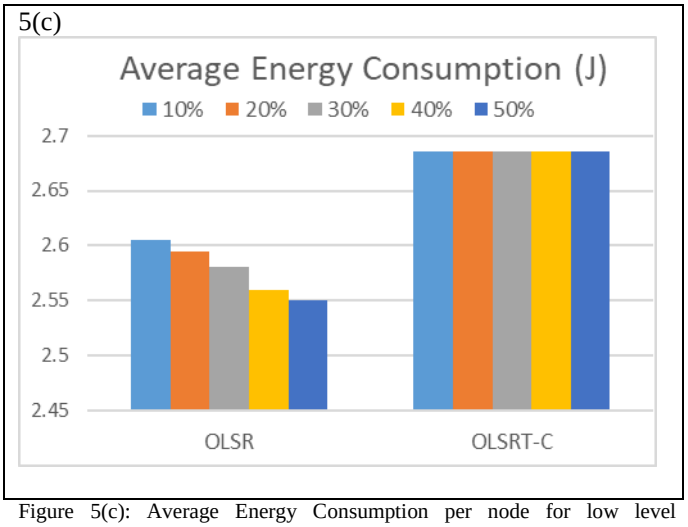


Figure 5(c): Average Energy Consumption per node for low level maliciousness, i.e. m_k=1

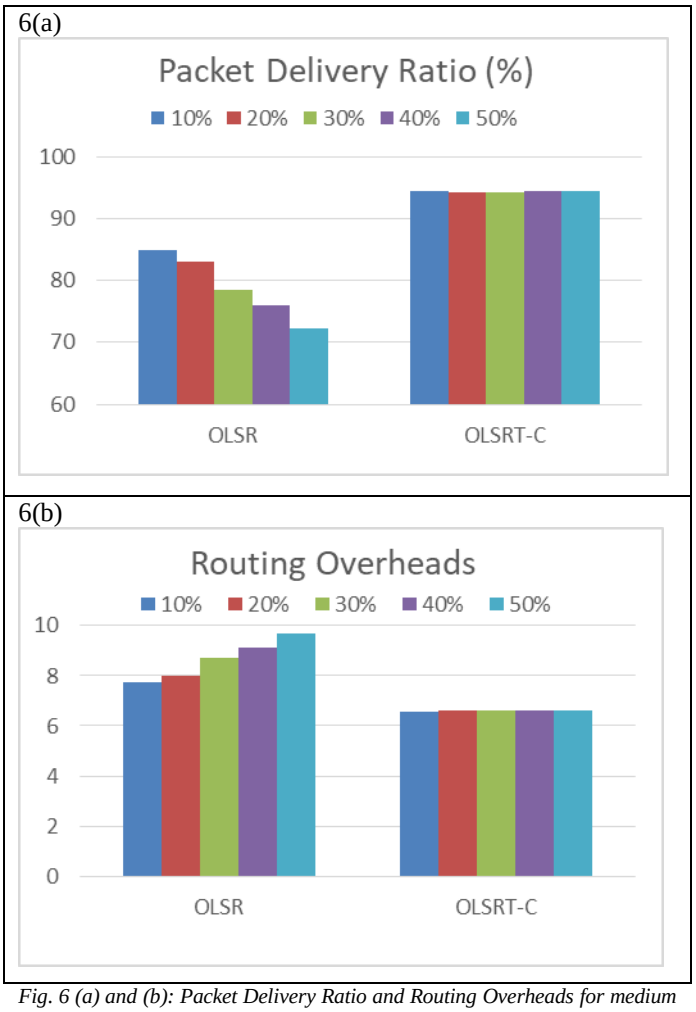


Fig. 6 (a) and (b): Packet Delivery Ratio and Routing Overheads for medium level maliciousness, i.e. m_k=2

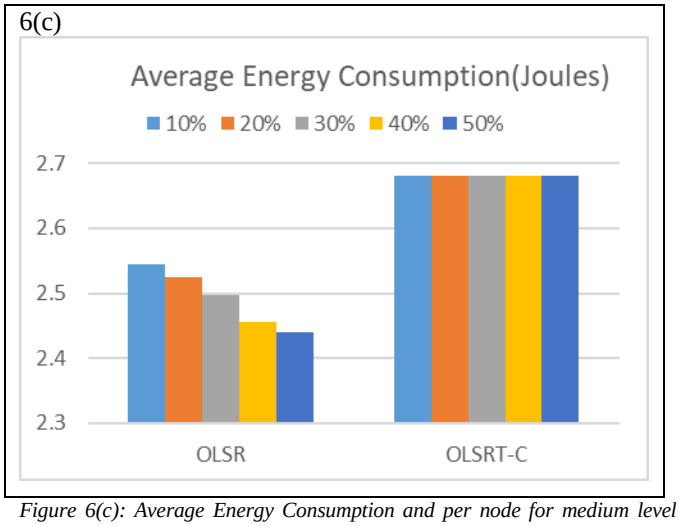


Figure 6(c): Average Energy Consumption and per node for medium level maliciousness, i.e. m_k=2

Table 2 and Table 3 indicate the simulation performance parameter comparison for low and medium level maliciousness respectively.

Table 2 Performance Parameters: Low level maliciousness

Percentage Malicious Nodes	OLSR			OLSRT-C		
	PDR (%)	RO	AEC (Joules)	PDR (%)	RO	AEC (Joules)
10%	91.64	5.48	2.6	96.03	4.89	2.68
20%	90.6	5.61	2.59	95.92	4.90	2.68
30%	88.07	5.99	2.57	95.96	4.90	2.68
40%	86.83	6.20	2.55	96.01	4.90	2.68
50%	84.76	6.51	2.54	95.98	4.90	2.68

Table 3 Performance Parameters: Medium level maliciousness

Percentage Malicious Nodes	OLSR			OLSRT-C		
	PDR (%)	RO	AEC (Joules)	PDR (%)	RO	AEC (Joules)
10%	84.98	7.76	2.54	94.45	6.58	2.67
20%	83	8.01	2.52	94.22	6.59	2.67
30%	78.4	8.73	2.49	94.32	6.60	2.67
40%	75.98	9.13	2.45	94.40	6.59	2.67
50%	72.21	9.71	2.44	94.35	6.60	2.67

It can be readily seen from table 2 that the PDR for normal OLSR gradually reduces from 91.64% to 84.76% as malicious presence increases from 10% to 50%. Compared to this modified OLSRT-C protocol provides improved PDR performance of 96% and this performance remains same for all percentages of malicious nodes. The table 2 also shows that for normal OLSR, RO gradually increases from 5.48 routing packets per data packet to 6.51 as malicious presence increases from 10% to 50%. As against this, with the OLSRT-C protocol RO reduces. The number of routing packets per data packet has been observed about 4.8 irrespective of level of malicious presence in the network. Thus OLSRT-C regulates the RO performance. The table 2

also shows that the AEC per node of the network reduces marginally from 2.6 Joules to 2.54 Joules, as the malicious presence increases from 10% to 50%. This can be expected as the overall energy consumption gets reduced with increase in malicious presence due to frequent ON-OFF switching of nodes in the network. With the use of OLSRT-C, AEC slightly increases, but it remains almost constant for all percentages of malicious nodes. This rise in AEC is because of number of alternative paths explored by OLSRT-C compared to the single and shortest path by OLSR protocol.

The table 3 shows the similar performance pattern for the medium level maliciousness for all three parameters, PDR, RO and AEC. However, the overall performance level gets further degraded in the medium level maliciousness. This is also an expected result, as frequency of nodes' ON-OFF switching significantly increases compared to low level maliciousness.

B. *Efficacy of protocols for Low Level and Medium level maliciousness SB attack:*

In order to consider the combined effect of the three parameters i.e. PDR, RO and AEC, the 'Efficacy' of the protocol has been defined as follows-

$$Efficacy = \frac{PDR}{N_C.RO} \quad (10)$$

In this equation, N_C represents Normalized Energy Consumption given by-

$$N_C = \frac{AEC}{E_0} \quad (11)$$

The figure 7 and figure 8 show the graphs for efficacy variation for both, normal OLSR and OLSRT-C protocols for low and medium level maliciousness respectively. It can be readily seen from figure 7 that for low level of maliciousness, the efficacy for normal OLSR protocol decreases from 64% to 51%, as the number of selfish nodes in the network increase from 10% to 50%. For the proposed OLSRT-C protocol, the efficacy is almost constant, approximately 73%, even if presence of malicious nodes in the network increases from 10% to 50%. This shows that the OLSRT-C protocol successfully mitigates the degradations due to random SB attack. Further, the stability of efficacy performance for OLSRT-C protocol for various percentages of malicious presence clearly indicates that OLSRT-C is also a robust protocol. Similar behavior can also be seen for medium level maliciousness from the figure 8, except that the overall efficacy performance itself degrades further. However, in this case, OLSRT-C provides significant improvement in efficacy performance compared to normal OLSR.

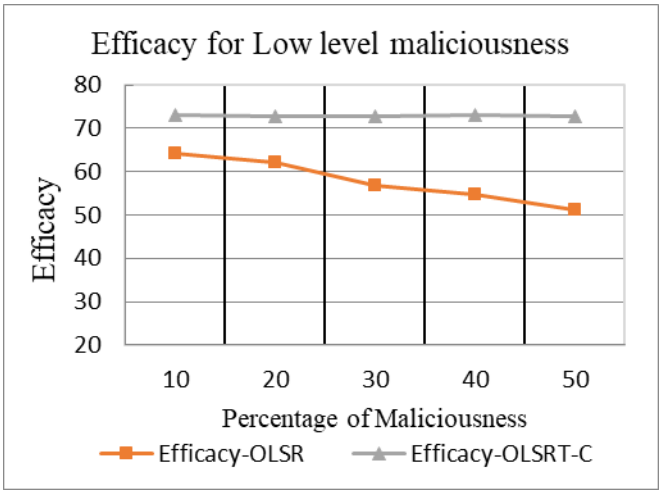


Figure 7 Efficacy comparison for low level maliciousness, i.e. m_k=1

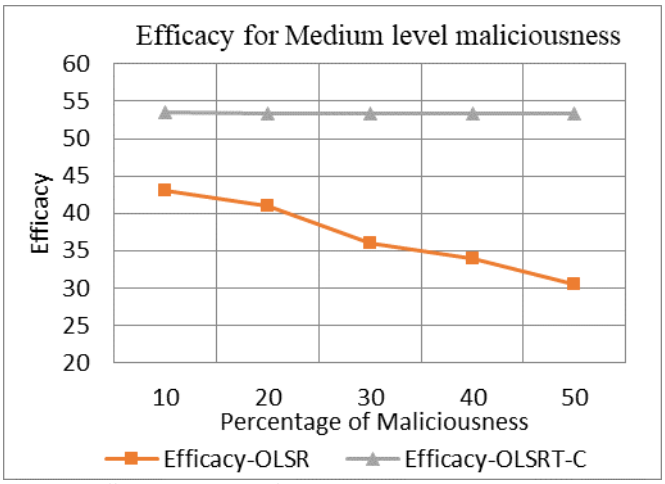


Figure 8: Efficacy comparison for medium level maliciousness, i.e. m_k=2

VI. CONCLUSION

In this paper, Trust-Confidence aware routing framework has been proposed and implemented for mitigating the effect of Selfish Behavior attack using OLSRT-C protocol. Exhaustive simulations have been carried out using ns-2. The results indicate that with the use of OLSRT-C routing protocol, the MANET data communication performance improves significantly. This is valid even if number of selfish nodes increases from 10% to 50% of total number of nodes in the network. The ROs performance also gets regulated appropriately and OLSRT-C provide a stable performance with marginal increase in AEC. As the efficacy for OLSRT-C protocol is higher compared to OLSR, it can be concluded that the mitigation of SB attack has been effectively achieved for the OLSRT-C protocol. Further, the performance almost remains constant, even if the malicious presence increases from 10% to 50%, which proves the robustness of the proposed OLSRT-C protocol.

In this paper, the Conditional Uniform Distribution has been used to model timing variations for random SB attack. This could be replaced by conditional single sided Laplacian distribution, as it may be more appropriate for causal situations. Even though the network performance has been simulated for a given network size of 1000m x 400m, the simulations can also be carried out with other network sizes such as, 500m x 500m or 1000m x 1000m or 5000m x 5000m, as may be encountered in different applications.

VII. REFERENCES

[1] T. Clausen, P. Jacquet*: "Optimized Link State Routing Protocol OLSR"*, IETF RFC-3626, 2003

[2] J. Wang, Y. Liu, Y. Jiao*: "Building a trusted route in a mobile ad hoc network considering Communication reliability and path length"*, Journal of Network and Computer Applications, 34(2011), pp. 1138-1149, 2011

[3] E. Perkins Charles, Bhagwat Pravin: *"Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers"*, SIGCOMM 94 -8/94 London England UK, 1994

[4] C. E. Perkins, E. M. Royer*: "Ad-hoc On-demand Distance Vector (AODV) Routing"*, IETF-RFC-3561, The Internet Society, 2003

[5] D. B. Johnson, D. A. Maltz: *"Dynamic Sources Routing (DSR) for Ad hoc Wireless Network"*, IETF RFC-4728, 2007

[6] A. Rajaram, S. Palaniswami: *"Malicious Node Detection System for Mobile Ad hoc Networks"*, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol.1, No.(2) , pp. 77-85, 2010

[7] K. A. Adoni, A. S. Tavildar: *"Probabilistic Modelling and Estimation of Network Blocking Probability for Selfish Behavior Attack in Mobile Ad hoc Networks*", IJCSN International Journal of Computer Science and Network,Vol.5, No.(4), pp. 653-659, August 2016

[8] K. A. Adoni, M. S. Karyakarte, A. S. Tavildar.: *"Security Framework for Black Hole Attack in Mobile Ad-hoc Networks"*, ICEIT National Conference on 'Advances in Mobile Communications, Networking and Computing', New Delhi, India, April 16-17, 2015, pp. 84-87, 2015

[9] Surya Aarohi: *"Modelling of Malicious Behavior due to Detour Attack in OLSR Protocol in MANET"*, Recent Researches in Electrical Engineering, pp. 276-283, 2014

[10] N. Suganthi, S. Neelavathy Pari,: *"Detecting Malicious Nodes in MANET using Rateless Codes for maximum content "*, 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, 17-19 December 2014, pp. 308-311, 2014

[11] Khaled Ahmed Abood Omer: *"The Impact of Node Misbehavior on the performance of Routing Protocols in MANET"*, International Journal of Computer Networks and Communications (IJCNC), Vol. 8, No.2, March 2016, pp. 103-112, 2016

[12] Umesh Kumar Singh, Jalaj Patidar and Kailash Chandra Phuleriya: *"On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks"*, International Journal of Scientific Research in Computer Science & Engineering, Volume 3, Issue 1, pp. 11-15, 2015.

[13] A.Vani: *"Detection and Elimination of Wormhole Attacks in a MANET"*, International Journal of Scientific Research in Computer Science & Engineering, Vol.5, Issue 5, pp-35-40, October (2017)

[14] Pradeep Kumar Sharma, Shivlal Mewada and Pratiksha Nigam: *"Investigation Based Performance of Black anf Gray Hole Attack in Mobile Ad-Hoc Network"*, International Journal of Scientific Research in Network Security and Communications, Volume-1, Issue-4, Oct. 2013

[15] S. Geetha, G. Geetha Ramani: *"Trust Model based on Bayesian Statistical method for AOMDV in MANET"*, Journal of Theoretical and Applied Information Technology, Vol. 69, No. 1, November 2014, pp. 172-181, 2014

[16] Zia Ullah, Muhammad Saleem Khan, Idrees Ahmed, Nadeem Javaid, Majid I. Khan,: *"Fuzzy Based Trust Model for Detection of Selfish Nodes in MANET"*, International Conference on Advanced Information Networking and Application, Crans Montana, Switzerland, 23-25 March 2016, pp. 965-972, 2016

[17] Janakiraman Sengathir and Rajendiran Manoharan*: "A futuristic trust coefficient-based semi-Markov prediction model for mitigating selfish nodes in MANETs"*, EURASIP Journal on Wireless Communications and Networking (2015) 2015:158, pp. 1-13, 2015

[18] Hui Xia, Zhiping Jia, Xin Li, Lei Ju, Edwin H.M. Sha: *"Trust Prediction and trust based source routing in mobile ad hoc networks"*, Ad Hoc Networks, 11(2013) pp. 2096-2114, 2013

[19] L. Odedra, A. Revar, M. H. Lunagaria: *"Detection and Prevention of Selfish Attack in MANET using Dynamic Learning"*, IOSR Journal of Computer Engineering (IOSR-JCE), Ver. V, May-Jun. 2016, Vol.18, No.(3), pp. 54-61, 2016

[20] M. Roy, C. Chowdhury, S. Neogy: *"Developing Secured MANET using Trust"*, Fourth ICACC International Conference on Advances in Computing and Communication, Cochin, India, 2014, pp. 183-186, 2014

[21] W. Gong, Z. You, D. Chen, et al.: *"Trust Based Malicious Nodes Detection in MANET"*, International Conference on E-business and Information Security, EBISS-2009, Wuhan, China, 2009

[22] G. Soni, K. Chandrawanshi*: "A Novel Defence Scheme against Selfish Node Attack in MANET"*, International Journal on Computational Sciences and Applications (IJCSA), June 2013, Vol.3, No.(3), pp. 51-63, 2013

[23] N. Kirubakaran, A. Kathirval: *"Performance Improvement of Security Attacks in Wireless Mobile Ad Hoc Network"*, Asian Journal of Information Technology, 2014, Vol.13, No.(2), pp. 68-76, 2014

[24] J. M. Singh, P. Josh Kumar, Ayyaswamy Kathirvel, N. Kirubakaran, P. Sivaraman, M. Subramanian*: "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT"*, EURASIP journal on Wireless Communication and Networking, 2015, 143, 2015

[25] D. G. Kampitaki, E. D. Karapistoli, A. A. Economides: *"Evaluating Selfishness Impact on MANETs"*, International Conference on Telecommunications and Multimedia (TEMU), Heraklion, Greece, 2014, pp. 64-68, 2014

[26] A. Banerjee, S. Neogy, C. Chowdhury*: "Reputation Based Trust Management System for MANET"*, Third International Conference on Engineering Applications of Information Technology (EAIT), Kolkata, India, 2012, pp. 376-381, 2012

[27] R. Venkataraman, M. Pushpalatha, T. R. Rao: *"Regression-based trust model for mobile ad hoc networks"*, IET Information Security, 2012, Vol.6, No.(3), pp. 131-140, 2012

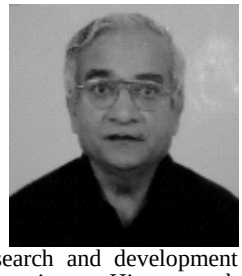
[28] K. A. Adoni, A. S. Tavildar*: "Trust aware routing framework for OLSR protocol to enhance performance of Mobile Ad-Hoc Networks"*, International Conference on Pervasive Computing (ICPC), Pune, India, Jan-2015, pp. 1-7, 2015

[29] K. A. Adoni, R. D. Joshi: *"Optimization of Energy consumption for OLSR routing protocol in MANE"*, International Journal of Wireless and Mobile Networks, India, February 2012, Vol.4, No.(1), pp. 251-262, 2012

[30] F. Bai, A. Helmy: *"A survey of Mobility Models in Wireless Adhoc Networks"*, Study – Grant NSF Career Award 0134650, University of Southern California, USA

Authors Profile

K. A. Adoni is presently working as Assistant Professor at P.E.S. Modern College of Engineering, Shivajinagar, Pune, India 411005. She is a Research Student of Electronics and Telecommunication Engineering department, V.I.I.T. Research Centre, Kondhwa, Pune, India 411048. She has completed her M.Tech. from Government College of Engineering, Pune, Maharashtra, India; in 2010. Her major fields of study are Wireless Networks, Mobile Ad-hoc Networks, Mobile Communication and Electronics System Design.



A. S. Tavildar was working as Emeritus Professor in Electronics and Telecommunication Engineering Department at VIIT Kondhwa, Pune, India. He has obtained his B.E. (Electronics and Telecommunication Engineering) from University of Pune and PhD (Communication Engineering) from Indian Institute of Technology, Delhi in 1984. He has 28 years of industrial, research and development experience and 16 years of teaching experience. His research interests are in signal processing, wireless and mobile communication systems. Prof Tavildar is Senior Member, IEEE USA, Fellow Member of IETE, India, Founder Member ICIET and Life Member of ISTE, India.

K. K. Warhade have completed B.E. (Electronics) and M.E. (Instrumentation) from Shri Guru Gobind Singhji Institute of Engineering and Technology Nanded, Maharashtra, India. He has completed his Ph.D. from Indian Institute of Technology Bombay (IIT Bombay), India. He has teaching experience of 22 years including 4 years research experience. He has published several papers in SCI Journals and reputed conferences. He also wrote book on "Video Shot Boundary Detection" published by River Publisher, Denmark. Currently he is working as a Professor in Electronics and Communication Engineering Department at MIT World Peace University, Pune, Maharashtra, India. His research interests are Video retrieval, Wavelets, Digital signal processing, Bio-medical signal and image processing, Filter design, Precision Agriculture and Wireless Communication.

