Wireless Pers Commun (2015) 81:961–979
DOI 10.1007/s11277-014-2165-5

# A Cooperative Routing for MANET Based on Distributed Trust and Energy Management

**U. Venkanna · Jeh Krishna Agarwal · R. Leela Velusamy**

Published online: 4 November 2014


**Abstract** A mobile ad-hoc network is an autonomous system having collection of mobile nodes connected by wireless links. Mobile nodes in a MANET communicate with each other based on unconditional cooperation and inherited trustworthiness. MANET is vulnerable due to the characteristics such as dynamic topology and openness. This leads to the exploitation of MANET by performing various kinds of attacks by the presence of malicious and (or) selfish nodes. Such nodes affect the normal routing process in a MANET thereby impacting the routing performances such as packet delivery ratio. Hence, the necessity of trust factor between communication nodes is substantiated. In this paper the proposed solution identifies the malicious and selfish behaviour of nodes by dynamic calculation of trust and energy values of the nodes in the topology. The proposed algorithm, Trust and Energy based Ad hoc On Demand Distance Vector improves the traditional AODV algorithm by the dynamic incorporation of trust and energy values for each node in the topology in order to achieve cooperative routing. In Trust and Energy based Ad hoc On Demand Distance Vector, the source node selects the cooperative path rather than the shortest path thereby isolating the malicious and selfish nodes. Finally, the simulation results show that the proposed Trust and Energy based Ad hoc On Demand Distance Vector routing algorithm isolate the malicious and selfish nodes, and substantially improves the routing performance such as packet delivery ratio and average end to end latency.

**Keywords** MANET · Trust management · Cooperative routing · AODV · AOTDV · TE-AODV

U. Venkanna (✉) · J. K. Agarwal · R. L. Velusamy
Department of Computer Science Engineering, National Institute of Technology, Tiruchirappalli 620 015, Tamil Nadu, India
e-mail: uvrao4u@gmail.com

J. K. Agarwal
e-mail: jeh.agarwal@gmail.com

R. L. Velusamy
e-mail: leela@nitt.edu

## 1 Introduction

In the last decade, advances in wireless networks have gathered great growth which has given rise to new research challenges. Mobile ad-hoc network is one of the wireless networks and infrastructure less networks. MANET is a collection of mobile nodes such as PDA, cell phones, mobile laptop which communicates over bandwidth constrained wireless links and performs operations such as route discovery, route maintenance in a self organized and cooperative way. MANET can be applied in situations where infrastructure cannot be deployed such as emergency applications, military field communications [1], commercial applications [2] and disaster management. In MANET each node acts like source and a router. In source node, a node generates its own traffic, whereas in a router a node receives the packets and relays them to next neighbour node.

Each node in mobile ad-hoc network communicates with the help of multi hop routing technique due to its limited communication range. Routing is a fundamental issue in MANET due to its characteristics. Routing in MANET can be categorized into proactive, reactive, and hybrid [3]. The basic routing protocol is in MANET such as DSDV [4], OLSR [5], AODV [6,7], and DSR [8]. These routing protocols are more vulnerable to routing attacks. To address the routing attacks secure routing protocols are such as SEAD [9], ARAN [10], and SAR [11] have been proposed. But these security routing protocols are based on Public Key Infrastructure, centralized trust authority and also dynamic key generation and distribution. Such infrastructures are difficult to provide in MANET environment. The cryptographic solutions are ineffective solutions in the presence of internal attacks and also have a serious impact on routing performance. To overcome the security problems in MANET, an alternate method based on Trust management has been proposed [12,13]. In Trust management, each node in the network topology is assigned a trust value based on the behaviour of the node. In a MANET, some nodes may behave as uncooperative node by dropping packets or modifying the packets due to dynamic changing behaviour. For this reasons nodes need to be monitored dynamically. Hence monitoring of nodes may be achieved by dynamic calculation of trust value and energy of each node. By using this trust value and energy value of nodes in the topology, a trustworthy route between source and destination can be established. In this paper the proposed solution calculates the trust value and remaining energy value to establish a trusted path between a source node and destination node. The main contributions of this work are twofold:

1. Dynamically calculate the trust and the remaining energy values for every node in the topology.
2. Establish a cooperative routing path using the trust and remaining energy values calculated.

The rest of the paper is organized as described below. Section 2 explains the problem statement. Section 3 gives the basic concepts of the Trust management model. Section 4 discusses the related work on trust based solutions for node misbehaviour in MANET. Section 5 explains the procedure to dynamically calculate trust and remaining energy values for each node and use it to establish the cooperative routing path between a source node and destination node. The simulation results and performance analysis are presented in Sect. 6. Finally, Sect. 7 gives the conclusion of this paper.

## 2 Problem Statement and Motivation

In MANET some nodes act as misbehaviour nodes [14,15]. The misbehaviour of nodes can be treated in two ways, viz., Malicious and selfish nodes. Malicious nodes are intentionally and actively misbehaving node which modifies the contents of the packet and disturbs the routing strategy of forwarding the packet. Due to the presence of malicious nodes several types of attacks such as Black hole attack [16–18], Gray hole attack [18,19], and Wormhole attacks are possible. Selfish nodes are positive behavioural nodes that are not cooperative in the data transmission process in order to save resources such as bandwidth and battery lifetime. Selfish nodes are ready to communicate with neighbour nodes only if it wants to send data packets. These selfish nodes seriously impact the packet delivery ratio and reliability of a MANET. Figure 1 shows the impact on the packet delivery ratio for a simulated MANET that uses an AODV routing algorithm and has misbehaviour nodes, for two different speeds (5 and 25 m/s). The simulation parameters considered is listed in Table 1. These malicious and selfish nodes need to be identified and eliminated to improve the routing performance in MANET. Hence, TE-AODV is proposed in this paper.

## 3 Background

### 3.1 Trust Management Model

Trust management is a method that can be used to improve the cooperative routing in a MANET. Cooperative routing improves the performance of MANET. In Trust management

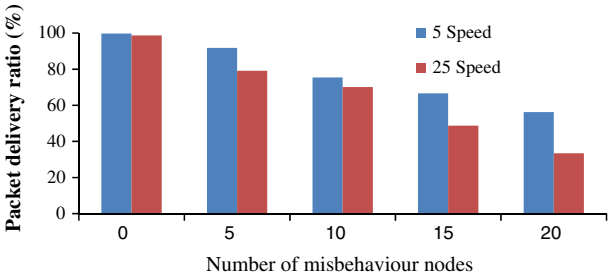
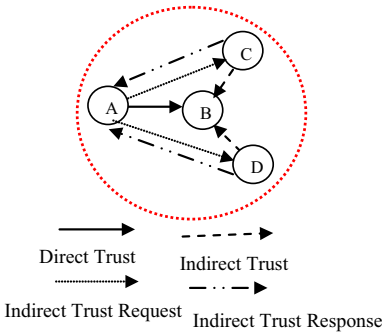



**Fig. 1** Impact of misbehaviour nodes on MANET

**Table 1** Simulation parameters

| Parameters | Value |
|---|---|
| Area | 1,000 m × 1,000 m |
| Total no. of nodes | 50 |
| Simulation time | 500 s |
| Transmission range | 250 m |
| Mobility model | Random way point |
| Maximum speed | 30 m/s |
| Mobility direction | Random |
| Pause time | 10 ms |
| Traffic type | Constant bit rating (UDP) |
| Number of connections | 20 |

**Fig. 2** Trust relationship types




a node calculates the trust value of its neighbour node by listening promiscuously. For calculating the trust value of the neighbour node the packet forwarding behaviour of the neighbour node is considered.

*Definition of Direct Trust and Indirect Trust Value*

The concept of Direct Trust and Indirect Trust has been used in pervasive computing, e-commerce application, and mobile ad hoc networks. To describe the terms Direct and Indirect trust consider the topology given in Fig. 2.

*Direct Trust Value (DTV)* Direct Trust of a particular node B is based on subjective assessment by the agent / peer node about the number of packets received and transmitted by node B at a given situation and given time. Direct trust is also defined as the degree of expectation of node A about node B to provide certain services.

*Indirect Trust Value (IDTV)* The Indirect trust of a node B is based on the perception of node B behaviour by nodes C and D based on its experiences and observations of node B past actions. These observations are conveyed in terms of recommendations to a particular node A.

Trust value of a node takes a value within the range 0–1. The trust value varies due to the dynamic behaviour of the nodes. Trust value 0 represents less trust worthy nodes and 1 represents more trustworthy nodes. Trust value having properties such as subjective, dynamic, asymmetric, and reflexive [20].

## 4 Related Work

This section discusses about cooperative and distributed trust models for secure routing in MANET.

Watch Dog and Pathrater mechanism [21] proposed a reputation trust management scheme that uses Watch Dog and Pathrater. WatchDog promiscuously listens to the behaviour of neighbour nodes, whereas Pathrater fixes the values for the behaviour of nodes within range 0–0.8 using WatchDog information. A node with value 0.5 fixed by Pathrater signifies the node as neutral. A node with value above 0.5 is classified as reliable otherwise it is malicious. The values fixed by the Pathrater are used to choose a reliable path from the source node to the destination node and eliminate the malicious nodes/selfish nodes in the path. During the route selection, the node with maximum value is always selected.

CONFIDANT (Cooperation of Nodes Fairness in Dynamic Ad-hoc Network) protocol [22] adds the trust manager and reputation modules to Watchdog and Pathrater. The trust manager evaluates the events reported by the Watchdog and disseminates ALARAM to other nodes in MANET regarding the misbehaviour of the nodes.

CORE divides the reputation of node into three different levels, viz., (a) subjective reputation: which is observed through nodes own observation, (b) indirect reputation: which are recommendations from neighbour nodes, (c) functional reputation: which is based upon the behaviour monitored by Watchdog during a specific task. These reputations are weighted and combined to calculate final reputation value of a node. The CORE scheme has two types of entities, viz., A requestor and a provider that are within wireless transmission range of the requestor. The requestor asks the providers for reputation values and validates the obtained results.

Attribute based similarity mechanism [24] is a model based on the degree of similarity between nodes. Each node determines trust value of neighbour nodes based on a set of attributes such as velocity, moving direction, encryption type, and affiliated organization. In this model, trusted routing scheme consist of four steps such as next hop determination, similarity degree calculation, packet transmission, and behaviour recognition.

Resnick and Zeckhauser [25] has proposed a distributed trust management method based on the authentication of messages, routes, and nodes. These mechanisms totally depend on the exchange of keys between the nodes and certificate signed by a Certificate Authority (CA).

Yang et al. [26] has made a performance comparison among trust based reactive routing protocols such as TAODV, TORA, and DSR, by varying different network parameters. The results show TORA performs better than other routing protocols in the presence of malicious nodes.

Li et al. [27] has proposed AOTDV based on Ad hoc on demand multi path routing protocol [28]. AOTDV identifies multiple paths between a source node and destination node based on trust vale and hop count. The trust value of the node is derived from two factors such as Control packet Forwarding Ratio (CFR) and Data packet Forwarding Ratio (DFR). The total path trust is computed as continuous product of nodes trust values.

## 5 Proposed Trust and Energy Based Ad hoc on Demand Distance Vector (te-aodv)

### 5.1 Assumptions

In our proposed model the following assumptions are made

1. Initially all the nodes in MANET are assigned the default direct trust value of 0.5.
2. The Final Trust Value of the node is in the range of [0, 1].
3. All the nodes in the network topology are operating in promiscuous mode.

### 5.2 Trust Model

The trust model used in the proposed algorithm calculates the Final Trust Value (FTV) of neighbour nodes by monitoring the neighbour node behaviour. FTV value can be calculated by using Direct and Indirect trust values. The algorithm for calculating FTV value is shown in Fig. 3.

#### *5.2.1 Direct Trust Value calculation (DTV)*

Each node in the network maintains the direct trust value of its neighbour nodes. The sender node after the transmission of any packet places itself in promiscuous mode to receive passive acknowledgement from immediate neighbours within the communication range of the

```
FTV_cal[B/A] ( )                    /* Node A calculates FTV value of neighbour Node B*/
{
  For every node in the topology initialize direct trust value as 0.5.
  Calculate DTV using the function DTV[B/A] ( );
   if(DTV[B/A] ≥ 0.5)
    α =1 and β=0
   else
   {
    α =0.5 and β=0.5
    IDTV[B/A] ( );
   }
 FTV[B/A] = α *DTV[B/A] + β*IDTV[B/A];
}
 DTV[B/A] ( )                       /* Function to calculate DTV of node B by node A*/
 {
  if (no interaction between node A and node B)
  then the direct value of node B is fixed to be 0.5
  else (interaction between node A and node B)
  {
   if(F (B) > D(B))                 /* F=Forwarding ratio D=Dropping ratio*/
   DTV_i[B/A]= DTV_i-1[B/A]+ (1- DTV_i-1[B/A])/20
   else
   {
     if (DTV[B/A] ≤ 0)
     DTV[B/A] = 0
     else
     DTV[B/A]= DTV_i-1[B/A]- (1- DTV_i-1[B/A])/10
   }
  }
 }
 IDTV[B/A] ( )                      /* Function to calculate IDTV of node B by node A*/
 {
  IDTV[B/A] = Σ_{i=1}^{N} RTV_i(B/n_i) / N      /* N is no of neighbour nodes*/
 }
```

**Fig. 3** Algorithm for FTV value calculation

wireless channel. Using this passive acknowledgement the sender node can calculate direct trust value of its neighbour node. Consider the topology given in Fig. 2. In Fig. 2 node A can calculate direct trust value of neighbour node B for fixed time intervals and updates the direct trust value of the neighbour node B at regular interval time ($\Delta$T) using the following two cases given below:

Case 1 : When F (B) > D (B) $\quad DTV_i\,[B/A] = DTV_{i-1}\,[B/A] + (1 - DTV_{i-1}[B/A])/20.$

Case 2 : When F (B) ≤ D (B) $\quad DTV_i\,[B/A] = DTV_{i-1}[B/A] - (1 - DTV_{i-1}[B/A])/10.$

For i varying from 1 to (Simulation time / $\Delta$T) and $DTV_0$ is initialized to 0.5. F(B) represents the number of successfully forwarded packet ratio by node B to its neighbour node, D(B) represents the dropped packet ratio of node B as monitored by node A, $DTV_i$ [B/A] represents a direct trust value of neighbour node B calculated by node A at time instant i. In case-1 if the forwarded ratio is greater than the dropped ratio, then the DTV of the neighbour node

increases by 5 % ((1 − $\mathrm{DTV_{i-1}}$ [B/A]) /20). In this case the DTV of the neighbour node keeps increasing monotonically in the range of 0.5–1. In case 2 if the dropped ratio is greater than the forwarded ratio, then the DTV of the neighbour node decreases by 10 % ((1 − $\mathrm{DTV_{i-1}}$ [B/A]) /10). In this case the DTV of the neighbour node keeps decreasing monotonically in the reverse range of 0.5–0.

### *5.2.2 Indirect Trust Value Calculation (IDTV)*

The IDTV of a node is calculated when a node does not have a DTV value greater than equal to 0.5. The node requests recommendations from the neighbour nodes.

$$\mathrm{IDTV\,[B/A]} = \sum_{i=1}^{N} \frac{RTV_i(B/n_i)}{N} \tag{1}$$

Where $RTV_i(B/n_i)$ represents recommended trust value of node B by the neighbour node $\mathrm{n_i}$. N represents the total number of recommendations received for node B.

### *5.2.3 Final Trust Value (FTV)*

The FTV of a node depends on both the direct trust value and the indirect trust value. The α part of DTV and β part of IDTV are used to calculate the FTV of a node B.

$$\mathrm{FTV\,[B/A]} = \alpha^{*}\mathrm{DTV\,[B/A]} + \beta^{*}\mathrm{IDTV\,[B/A)\ \ such\ that}\ \alpha + \beta = 1. \tag{2}$$

Where α takes a value of 1 when DTV[B/A] ≥ 0.5 and β takes value as 0.

Where α takes a value of 0.5 when DTV[B/A] < 0.5 and β takes value as 0.5.

## 5.3 Energy Value Calculation

Every mobile node in MANET consumes energy to transmit a packet, receive a packet and overhear the neighbour nodes. The energy consumed at a particular node ($\mathrm{n_x}$) is calculated as follows:

$$\begin{aligned}
\mathrm{E\,(n_x)_{consumed}} &= \mathrm{E\ (n_x)_{Transmission}} + \mathrm{E\,(n_x)_{Reception}} \\
&\quad + (\mathrm{N}-1)^{*}\,\mathrm{E\,(n_x)_{overhearing}} \\
\mathrm{E\,(n_x)_{remaining\ energy}} &= \mathrm{E\,(n_x)_{inital\ energy}} - \mathrm{E\,(n_x)_{consumed\ energy}} \\
\mathrm{E\,(n_x)_{remainig_energy_percentage}} &= \frac{E(\mathrm{n_x})remaing\ energy}{E(\mathrm{n_x})initial\ energy} \times 100
\end{aligned} \tag{3}$$

Where N is the number of neighbouring nodes of $\mathrm{n_x}$. The energy value of a mobile node is calculated at regular intervals to determine the remaining energy and in turn to calculate the remaining energy percentage. If the remaining energy percentage for a node is greater than equal to 50 % the node energy level is assigned with a value of 1 else 2. Once the mobile node energy level gets reduced to 2, it will broadcast an Energy_Level message. The format of the message is given below:

| Bytes: | 1 | 1 |
|---|---|---|
| | Node_ID | Energy_ Level |

In Fig. 2 each node stores the information about FTV and remaining energy level of its neighbour nodes in the Neighbour Node (NN) table. The cooperative node to forward the

packets is selected using the information in the NN table. The format of the entries in the NN table is given below:

| N_ID | FTV | Energy Level |
|---|---|---|

### 5.4 Cooperative Route Selection

Reactive routing protocol (AODV) dynamically establishes the route from source node to the destination node. In our proposed solution an effective cooperative route between a source node and destination node is calculated by considering the final trust value and remaining energy of neighbour nodes. Cooperative routing in MANET basically consist of two major phases as listed below:

1. Route discovery and best route selection
2. Route maintenance

#### *5.4.1 Route Discovery and Best Route Selection*

The route discovery process is initiated by the source node. Initially a source node will check the routing table for an Existing Route (ER) to the destination. If a route exists from the source node $n_1$ to destination node $n_N$ with intermediate nodes along the route $n_2$, $n_3$, …, $n_{N-1}$. The source node generates Trusted Route Request (TRREQ) and forwards according to ER in the routing table. The destination in ER calculates Average trust value for the existing route $T_{Avg}$(ER) is using Eq. 4 and generates Trusted Route Reply (TRREP) forwarded to the source node. If $T_{Avg}$(ER) is more than the set threshold value (threshold value set as per simulation scenario), then the existing route is selected else route discovery is initiated.

The format for TRREQ message is given below:

Bytes: 4 4 4 1 1

| Broadcast ID | Source Address | Destination Address | HopCounter | Total_Trust |
|---|---|---|---|---|

The format for TRREP message is given below:

Bytes: 4 4 4 1 1

| Destination Address | Source Address | Life Time | Total_Trust | $T_{Avg}$(ER) |
|---|---|---|---|---|

$$T_{Avg}\,(ER) \quad = \sum_{i=1}^{N} \left( \frac{FTV\left(\frac{n_i+1}{n_i}\right)}{N} \right) \tag{4}$$

Where N is the number of hops along the ER and $FTV\left(\frac{n_i+1}{ni}\right)$ is the FTV of node $n_{i+1}$ calculated by $n_i$.

Route discovery and best route selection consist of three phases

1. RREQ
2. RREP
3. Best route selection

*Route Request (RREQ)*

The source node broadcasts a RREQ to its neighbours. The format of the RREQ packet is given below:

| Bytes: | 4 | 4 | 4 | 4 | 4 | 1 | 1 |
|---|---|---|---|---|---|---|---|
| | Broad cast ID | Destination Address | Destination Seq_no | Source Address | Source Seq_no | Hop Counter | Total_Trust |

On receiving the RREQ packets, the neighbour nodes check for availability of a route in its routing table. If a trusted route exists, it will reply with a RREP message else it selects from its NN table all nodes having final trust value and remaining energy value greater than 0.5.

The RREQ packet is modified (FTV value of neighbour node is added to Total_Trust value in RREQ packet) and forwarded to each selected neighbours respectively. If the NN table does not have any node with final trust value and remaining energy value greater than 0.5 the RREQ packet is dropped. The RREQ algorithm is given in Fig. 4.

**RREQ ( )**
{
Initially source node check for ER in its routing table
**if** (ER exists in routing table)
{
Source generates TRREQ add the next node FTV value to the **Total_Trust** value in the received TRREQ, increments the **HopCounter,** then forward the modified TRREQ to its next node in the ER.
Repeat the process at each node along the ER until the destination reached
Destination node calculates $T_{Avg}(ER)$ by using Equation $\sum_{i=1}^{N}\left(\frac{FTV\left(\frac{n_{i+1}}{n_i}\right)}{N}\right)$ and generates TRREP, then forwards to source node according to reverse route entry in the routing table.
}
**if** ($T_{Avg}(ER)$ > Threshold trust value)
{
ER is selected and source node start sending data to destination node.
}
**else**
{
Broadcast RREQ.
Intermediate neighbour nodes receive RREQ.
**if** ( intermediate node has processed RREQ with same **Broadcast ID** )
Drop RREQ with that particular **Broadcast ID.**
**else**
{
Check in its NN table for its neighbours FTV and remaining energy value.
**if** (FTV and remaining energy value > 0.5)
{
Add the next node FTV value to the **Total_Trust** value in the received RREQ, increments the **HopCounter,** then forward the modified RREQ to its neighbours.
Repeat the process at each node along the discovered path until the destination reached.
}
**else**
Drop RREQ.
}
}
}

**Fig. 4** RREQ algorithm

*Route Reply (RREP)*

Destination node will receive one (or) more RREQ. After receiving the first RREQ destination will set timer $T_e$. If $T_e$ value expires the remaining RREQ packets are dropped. For all the received RREQ packets, RREP packets are generated and sent to the source node. The format of RREP message is given below:

| Bytes: | 4 | 4 | 4 | 1 | 4 | 1 | 1 |
|---|---|---|---|---|---|---|---|
| Destination Address | Destination Seq_no | Source Address | Hop Counter | Life Time | $T_{Avg}$(NR) | Total_Trust | |

$\mathbf{T}_{Avg}$ value in RREP packet calculated using Eq. 5.The RREP algorithm is given in Fig. 5.

$$T_{Avg}\,(NR) \quad = \sum_{i=1}^{N} \left( \frac{FTV\left(\frac{n_i+1}{n_i}\right)}{N} \right) \tag{5}$$

Where N is the number of hops along the NR and $FTV_i$ is the FTV of node $n_{i+1}$ calculated by $n_i$.

*Best Route Selection*

Source node will receive multiple RREP from the destination. After receiving first RREP, the source will set timer $T_e$, if $T_e$ value expires, source node will drop the remaining RREP. From the received RREP the source will select the best route based on $T_{Avg}$ Value. The algorithm for best route selection is given in Fig. 6.

**RREP ( )**
{
The destination node will set timer $T_e$, after the receiving the first RREQ.
**if** ($T_e$ = 0)
{
Destination node drops next RREQ, then
Destination node calculates $T_{Avg}$(NR) by using Equation $\sum_{i=1}^{N} \left( \frac{FTV\left(\frac{n_{i+1}}{n_i}\right)}{N} \right)$ and
generates RREP.
Destination forwards RREP to the source node with reverse route entry in routing table.
}
}

**Fig. 5** RREP algorithm

**Bestroute_selection ( )**
{
The source node will set Timer $T_e$ , after receiving first RREP.
**if** ($T_e$=0) then
{
The source node drops the next RREP.
Among the RREP received to the source node selects best route having high $T_{Avg}$ value.
Source node starts sending data using the selected route to destination node.
}
}

**Fig. 6** Best route selection algorithm

#### *5.4.2 Route Maintenance*

Route maintenance is mainly used for two purposes such as when a link is broken between two mobile nodes due to mobility and The FTV of the mobile node is modified due to its behaviour. In situations when a link is broken or the lifetime of the route gets expired, then the RERR notification is sent to the source node. In situations when the FTV value of mobile node gets reduced to value of 0.5 or less, the RERR notification is sent to the source node. On receiving RERR notification the source node discovers a new route to the destination node.

## 6 Simulation and Results Analysis

The proposed TE-AODV routing algorithm was developed and tested using the Ns-2 simulator [29]. The algorithm was simulated using the parameters listed in Table 1.

### 6.1 Performance Parameters

To analyse the performance of the proposed algorithm three different simulation scenarios and four different metrics were considered. The performance metrics considered for the various test cases are listed below:

1. *Packet delivery ratio* the ratio of packets received by destination node to those sent by the source node.
2. *Average end-to-end latency* the average time taken by data packets to reach destination which includes buffer delay during a route discovery, queuing delay at the interface, retransmit delay at the MAC layer, and propagation delay.
3. *Routing packet overhead* ratio of control packets (includes RREQ/RREP/RERR TTREQ/TRREP) generated to the total number of data packets sent.
4. *Energy consumption* energy consumption per second during the simulation time.

### 6.2 Result Analysis

In our simulation scenario, fifty nodes were randomly scattered in 1000m × 1000m rectangle area. The total simulation time was set to 500 s. The transmission range of every node in one hop was fixed at 250 m. The random waypoint mobility model was chosen in which each packet starts its journey from random source to random destination with maximum speed of 30 m/s and mobility direction was also set at random. The IEEE 802.11 Distributed Coordinate Function (DCF) was used as the Medium Access Control (MAC) protocol. Some nodes were randomly selected as malicious nodes to launch the Blackhole attack and Grayhole attack.

To study the various behaviour of the nodes a simulation experiment was conducted. The behaviour of a node was measured in terms of dynamic calculation of final trust value. Six nodes (1, 4, 16, 24, 30, 40) were randomly selected and the final trust value for each node was calculated at regular intervals of 100 s for about 500 s of simulation time. During the simulation, nodes numbered 1, 30, and 40 was forcefully made to be misbehave by performing Black hole and Gray hole attacks, whereas nodes numbered 4, 16, and 24 are retained as cooperative nodes. The final trust value obtained for the six nodes during the simulation study is plotted as the graph in Fig. 7. From Fig. 7 it is observed that the trust value of nodes 1, 30, and 40 monotonically decreases to zero due to the misbehaviour of nodes. The final trust value of nodes 4, 16, and 24 monotonically increases to 0.999 due to the cooperative behaviour of these nodes. The performance of proposed routing algorithm TE-AODV was

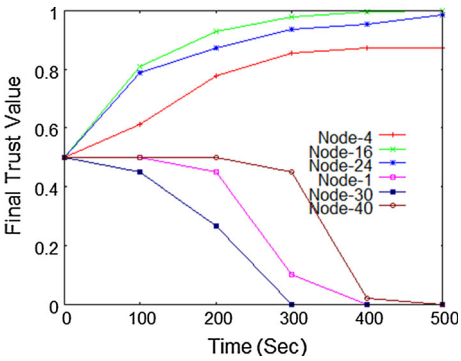



**Fig. 7** Final trust values of different nodes

**Table 2** Varying simulation parameters

| Scenario | Number of malicious nodes | Speed | Trust update threshold |
|---|---|---|---|
| 1 | 10 | 0–30 | 0.05 |
| 2 | 0–20 | 10 | 0.05 |
| 3 | 10 | 10 | 0.02–0.1 |

studied for three different simulation scenarios. Table 2 lists the various scenarios for which the simulation study was done.

In the first scenario the speed of the nodes was varied from 0 to 30 m/s. In the second scenario the number of malicious nodes was varied between 0 and 20. The time period for observing the FTV for nodes is said to be trust update threshold. In the third scenario trust update threshold was varied 0.02–0.1 s.

Sections 6.2.1–6.2.3 discusses the performance of the proposed TE-AODV routing algorithm with respective packet delivery ratio, the average end-to-end latency, routing packet overhead, and energy consumption and compares it with AODV and AOTDV routing algorithm for the following three scenarios.

### *6.2.1 Scenario 1 with Varying Node Speeds*

In this scenario the speed of the mobile nodes was varied between 0 and 30 m/s. The effect of the speed of mobile nodes on the performance parameters such as a packet delivery ratio, the average end-to-end latency, routing packet overhead, and energy consumption was observed and plotted as graphs shown in Fig. 8.

Figure 8a represents the graph plotted for node speed versus packet delivery ratio for the AODV, AOTDV and TE-AODV routing algorithms. It can be seen from Fig. 8a that the packet delivery ratio of the TE-AODV remains higher across the varying speed of mobile nodes in comparison with AODV and AOTDV. While establishing a path, TE-AODV selects its neighbour node based on the higher value of FTV and remaining energy. This establishes a cooperative path between sender and receiver; thereby eliminating the malicious and selfish nodes through the path. Hence, the dropping of packets by intermediate nodes is less, thereby increasing the packet delivery ratio. In case of AODV, the behaviour of the node is not considered while establishing the path. Hence, more number of packets are dropped by malicious and selfish nodes if a path uses them. Therefore the packet delivery ratio reduces considerably. In case of AOTDV the remaining energy value of the node is not considered

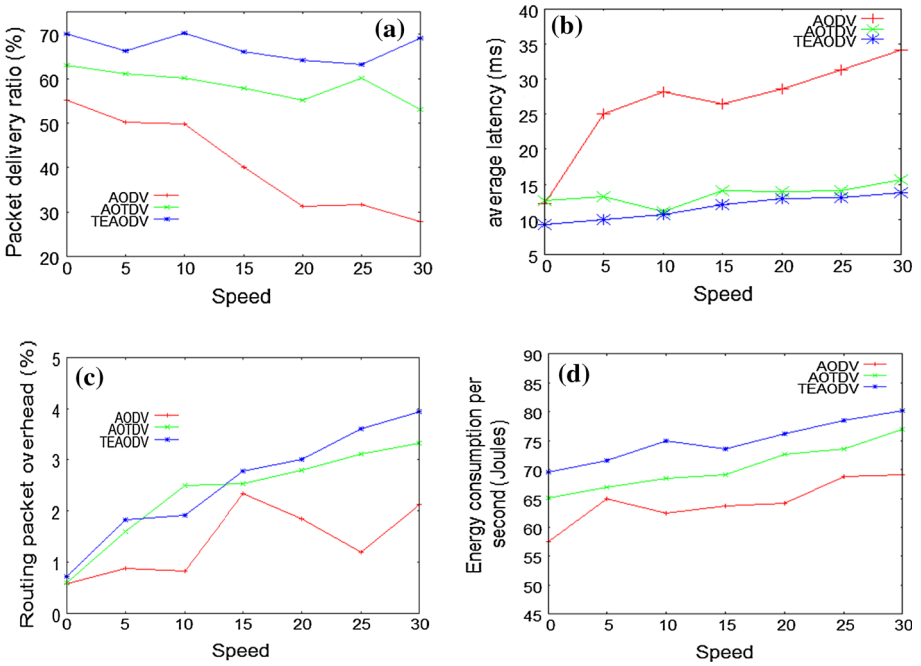



**Fig. 8** Scenario 1 Performance parameters with varying node speed. **a** Packet delivery ratio. **b** Average latency. **c** Routing packets overhead. **d** Energy consumption

while establishing a path from source to destination. Therefore there is a possibility for selfish node (less remaining energy) to occur in the path. Hence the result in reduction of the packet delivery ratio compared with TE-AODV.

Figure 8b represents the graph plotted for node speed versus average end to end latency for the AODV, AOTDV and TE-AODV routing algorithms. From Fig. 8b it can be observed that the average end to end latency of a packet to transmit in MANET is directly proportional to the speed of the node. This is due to the frequent changing route entries in the routing table. In AODV algorithm, the average end to end latency keeps increasing because, the presence of malicious and selfish nodes in the path found by AODV. These nodes drop the packets and therefore more retransmission needs to be done. In TE-AODV the elimination of malicious and selfish nodes from the path using FTV and remaining energy reduces the number of packets dropped thereby reducing average end to end latency when compared with AODV and AOTDV. AOTDV considers the weighted Control Forwarding Ratio (CFR) for calculating trust value. This calculation of CFR is ineffective in meeting the required trust value for establishing an optimal path, leading to an increase in average end to end latency in comparison with TE-AODV.

Figure 8c represents the graph plotted for node speed versus routing packet overhead for the AODV, AOTDV and TE-AODV routing algorithms. In AODV the routing overhead is less compared with AOTDV and TE-AODV. This is due to less transmission of control packet (RREQ, RREP) to establish a path. In TE-AODV, for establishing a cooperative path extra control packet pair such as RREQ-RREP, TRREQ-TRREP are used. These control packets increases the routing overhead in TE-AODV. From the Fig.8c, the average routing overhead for AOTDV and TE-AODV are 2.35 and 2.54 % respectively. It can be seen that there is a marginal increase of 0.19 % in the TE - AODV compared with AOTDV.

Figure 8d represents the graph plotted for node speed versus energy consumption for the AODV, AOTDV and TE-AODV routing algorithms. Energy consumption of a mobile node in MANET is consumed for processing of control and data packets. In AODV, energy is consumed mainly for transmitting and reception of packets. But in AOTDV and TE-AODV, the energy consumption is more due to promiscuous listening of neighbouring nodes for monitoring the behaviour. In TE-AODV, energy consumption is marginally higher than AOTDV due to extra processing of control packets. From the Fig. 8d the average energy consumption for AOTDV and TE-AODV are 70.39 and 74.90 J/s respectively. The extra average energy consumption 4.5 J/s in TE-AODV in comparison with AOTDV.

### *6.2.2 Scenario 2 with Varying Number of Malicious Nodes*

In this scenario the number of malicious nodes was varied between 0 and 20. The effect of the varying number of malicious nodes on the performance parameters such as a packet delivery ratio, the average end-to-end latency, the routing packet overhead, and energy consumption was observed and plotted as graphs shown in Fig. 9.

Figure 9a represents the graph plotted for a number of malicious nodes versus packet delivery ratio of the AODV, AOTDV, and TE-AODV routing algorithms. It can be seen from Fig. 9a that the packet delivery ratio of proposed TE-AODV remains high compared with AOTDV by varying the number of malicious nodes. The reason is that, dynamic calculation of FTV and remaining energy of a node reflects the changing behaviour of the nodes from benevolent to malicious and selfish nodes. This helps elimination of malicious and selfish nodes in the routing path which in turn reduces the number of dropped packets. In AODV

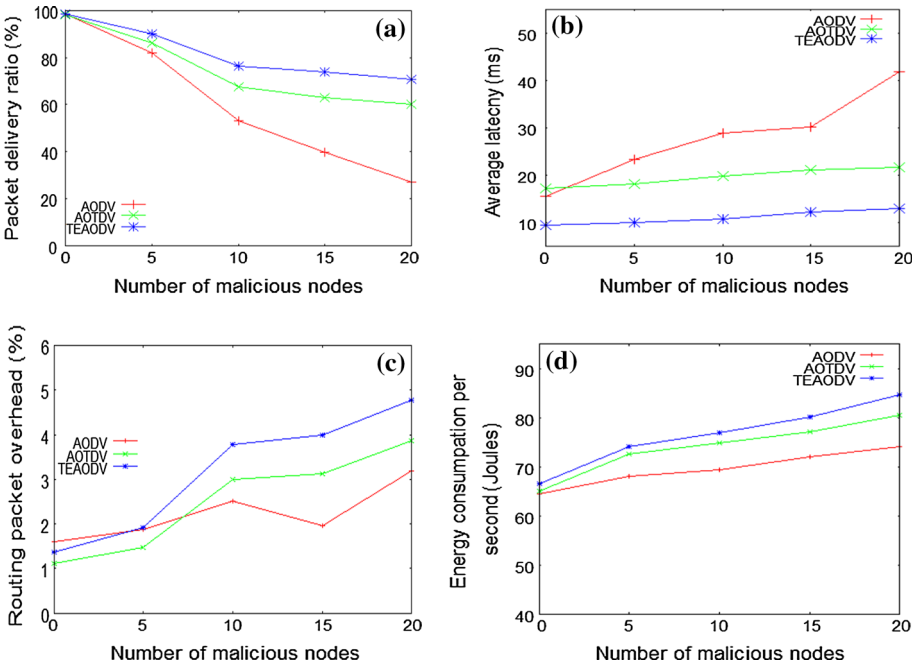



**Fig. 9** Scenario 2 Performance parameters with varying number of malicious nodes. **a** Packet delivery ratio. **b** Average latency. **c** Routing packets overhead. **d** Energy consumption

the routing path between source and destination node consist of malicious and selfish nodes; thereby more packets dropped, hence packet delivery ratio degrades remarkably as the number of malicious nodes increases. Because of this AODV packet delivery ratio is less compared with AOTDV and TE-AODV.

In case of AOTDV the presence of malicious nodes in the routing path does not alter the trust value of the node with respective dynamic changing behaviour node. This increases the possibility of retaining the malicious nodes in the path. Hence the packet delivery ratio is less in comparison with TE-AODV.

Figure 9b represents the graph plotted for number of malicious nodes versus end to end latency of the AODV, AOTDV, and TE-AODV routing algorithms. It can be seen from Fig. 9b the average end to end latency for AODV is high when compared with AOTDV and TE-AODV. Once again this is due to the presence of malicious and selfish nodes in the path identified by AODV. These nodes drop packets and more retransmission of packets occurs. In TE-AODV the elimination of malicious and selfish nodes reduces the number of retransmissions, thereby reducing the average end to end latency compared with AOTDV. In case of AOTDV, the weighted calculation of trust value of a node increases the number of hops between source and destination node, thereby average end to end latency is high in comparison with TE-AODV.

Figure 9c represents the graph plotted for number of malicious nodes versus routing packet overhead for AODV, AOTDV, and TE-AODV routing algorithms. The routing packet overhead for AODV is less when compared with AOTDV and TE-AODV. This is due to less broadcasting of control packets (RREQ/RREP). From Fig. 9c the average routing overhead for AOTDV and TE-AODV are 2.51, 3.16 % respectively. It can be seen that there is a marginal increase of 0.65 % in the TE-AODV. The reason is that the more number of the RREQ / RREP, TRREQ/TRREP broadcasts is to establish a required cooperative route.

Figure 9d represents the graph plotted for number of malicious nodes versus energy consumption for AODV, AOTDV and TE-AODV routing algorithms. There is a reduction in the energy consumption with AODV compared to AOTDV and TE-AODV. This is due to less number of control packets are processed. In TE-AODV, energy consumption is marginally higher than AOTDV due to extra processing of control packets and monitoring of neighbour Nodes for establishing a cooperative path. From Fig. 9d the average energy consumption for AOTDV and TE-AODV are 74.07 and 76.52 J/s respectively. The extra energy consumption of TE-AODV compared with AOTDV is 2.45 J/s.

### *6.2.3 Scenario 3 with Varying Trust Update Threshold*

In this scenario the trust update threshold value was varied between 0.02 and 0.1 s. The effect of trust update threshold interval on the performance parameters such as a packet delivery ratio, the average end-to-end latency, the routing packet overhead, and energy consumption was observed and plotted as graphs shown in Fig. 10.

Figure 10a represents the graph plotted for varying trust update threshold versus packet delivery ratio for the AOTDV and TE-AODV routing algorithms. From Fig. 10a it can be seen that the packet delivery ratio of TE-AODV remains high across the varying trust update threshold. This is due to establishing more trust worthy route by frequent updating of the trust value of its neighbouring nodes, thereby increasing the packet delivery ratio. The updating of trust value of a node is gradually incremented by 0.02. This constraint in reaching the required trust for the path establishment is difficult. As a trust update threshold increases, there is possibility of less trustworthy nodes in the path there by decreasing the packet delivery ratio hence, the packet delivery ratio for AOTDV is less comparison with TE-AODV.

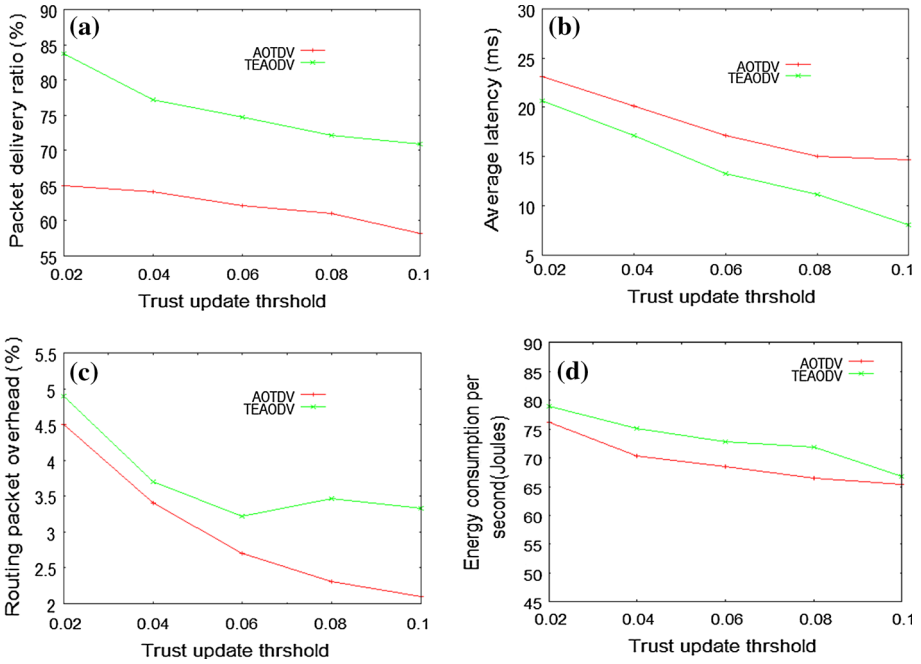



**Fig. 10** Scenario 3 Performance parameters with varying trust update threshold. **a** Packet delivery ratio. **b** Average latency. **c** Routing packets overhead. **d** Energy consumption

Figure 10b represents the graph plotted from varying trust update threshold versus end to end latency for AOTDV and TE-AODV routing algorithms. It can be seen that for increasing values of trust threshold, the average end to end latency for AOTDV and TE-AODV was decreasing. This is due to delays incurred in the routing path. In TE-AODV, for cooperative nodes, the trust value increases gradually. This ensures that the node is always maintained in the selected cooperative path. Hence, the average end to end latency incurred less in the path to transmit a packet. This improvement in trust value calculation reduces the end to end latency than the AOTDV.

Figure 10c represents the graph plotted for varying trust update threshold versus routing packet overhead for AOTDV and TE-AODV routing algorithms. The routing overhead for AOTDV and TE-AODV decreases slowly with increase of trust update threshold. The reason is that, for frequent updating of trust value of threshold (0.02), the number of control packets for cooperative route establishment increases. This ensures the maintenance of more cooperative nodes in the NN table. When the updating of trust value threshold is less frequent (0.1), the number of control packets for cooperative establishment decreases. This can lead to maintenance of less trustworthy nodes in the NN table; and hence affects the routing performance. From Fig. 10c the average routing overhead for AOTDV and TE-AODV are 3, 3.72 % respectively. It can be seen that there is a marginal increase of 0.72 % in the TE-AODV algorithm. This increase is due to frequent broadcasting control packets (RERR/TRREQ-TRREP) when the variation in trust value of a node.

Figure 10d represents the graph plotted for varying trust update threshold versus energy consumption for AOTDV and TE-AODV routing algorithms. From Fig. 10d the average energy consumption for AOTDV and TE-AODV are 69.36 and 73.08 J/s respectively. The

**Table 3** Performance comparison of various routing algorithms

| Performance parameters | Routing algorithms | | |
|---|---|---|---|
| | AODV | AOTDV | TE-AODV |
| Average packet delivery ratio (%) | 50.15 | 65.25 | 74.91 |
| Average end to end latency (ms) | 27.05 | 17.03 | 13.04 |
| Average routing packet overhead (%) | 1.08 | 2.62 | 3.14 |
| Average energy consumption (J) | 67.02 | 71.28 | 74.83 |

extra energy consumption of 3.72 J/s in TE-AODV is due to processing of extra routing packet overhead(RERR/ RREQ-RREP/TRREQ-TRREP) and calculation of IDTV.

### 6.3 Summary of Experiments

Table 3 shows the comparative performance of AODV, AOTDV, and TE-AODV routing algorithms. To summarize the performance of TE-AODV, the increase in the packet delivery ratio and average end to end latency is mainly due to the accurate elimination of malicious and selfish nodes in the path formed by TE-AODV. By elimination of malicious and selfish nodes retransmission of packets reduced, which in turn increase the packet delivery ratio and reduce the average end to end latency. However there is considerable increase in routing overhead and energy consumption due to the introduction of extra control packet pairs such as RREQ-RREP a TRREQ-TRREP, RERR, and calculation of IDTV of a node, the average routing overhead marginally increases. This in turn increases the average energy consumption of TE-AODV.

## 7 Conclusion

In this paper, distributed trust and energy management model for dynamic routing has been proposed. The proposed model calculates the FTV value and the remaining energy value for the nodes in a MANET. These calculated values are used to establish a cooperative and reliable path between a source node and destination node. To analyse the performance of proposed TE-AODV routing algorithm, a simulation study was conducted with three different scenarios. The TE-AODV was compared with AODV, AOTDV in terms of Packet delivery ratio, Average end to end latency, routing packet overhead and energy consumption. From the results it was found that the TE-AODV performs better than the existing algorithms with respect to the packet delivery ratio and end to end latency. However there is a marginal increase in routing overhead and energy consumption are manageable.

## References

1. Toumpis, S., & Toumpakaris, D. (2006). Wireless ad hoc networks and related topologies: Applications and research challenges. *Elektrotechnik and Informationstechnik*, *123*(6), 232–241.
2. Huang, E., Hu, W., Crowcroft, J., & Wassell, I. (2005). Towards commercial mobile ad hoc network applications: A radio dispatch system. In *MobiHoc'05*, pp. 355–365.
3. Boukerche, A., Turgut, B., Aydin, N., Ahmad, M. Z., Bölöni, L., & Turgut, D. (2011). Routing protocols in ad hoc networks: A survey. *Computer Networks*, *55*(13), 3032–3080.

4. Perkins, C., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *Proceedings ACM SIGCOMM*, pp. 234–244.
5. Clausen, T., Jacquet, P., Laouiti, A., Muhlethaler, P.,Qayyum, A., & Viennot, L. (2001). Optimized link state routing protocolfor ad hoc networks. In *Proceedings IEEE INMIC*, pp. 62–68.
6. Perkins, C. E., & Roye, E. M. (1999). Ad-hoc on-demand distance vectorrouting. In *Proceedings the mobile computing systems and applications*, pp. 90–100.
7. Perkins, C. E. (2003). Ad-hoc on-demand distance vector routing. RFC 3561, July.
8. Johnson, D., Hu, Y., & Maltz, D. (2007). The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. February; rfc4728.
9. Hu, Y.-C., Johnson, D.B., & Perrig, A. (2002). Secure efficient distance vector routing in mobile wireless ad hoc networks. In *Proceedings of IEEE workshop mobile computing systems and applications*, pp. 3–13.
10. Sanzgiri, K. et al. (2002). Authenticated routing for ad hoc networks. In *Proceedings of 10th IEEE international conference on network protocols*, pp. 78–87.
11. Yi, S., Naldurg, P., & Kravets, R. (2001). Security-aware ad hoc routing for wireless networks. In *Proceedings of ACM international symposium. on mobile ad hoc networking and computing*, pp. 299–302.
12. Marchang, N., & Datta, R. (2012). Light-weight trust-based routing protocol for mobile ad hoc networks. *IET Information Security*, *6*(2), 77–83.
13. Wang, B., Huang, C. H., Li, L. Y., & Yang, W. Z. (2011). Trust based minimum cost opportunistic routing for Ad Hoc networks. *Journal of Systems and Software*, *84*(12), 2107–2122.
14. Hollick, M., Schmitt, J., Seipl, C., & Steinmetz, R.(2004). On the effect of node misbehavior in ad hoc networks. In *Proceedings of IEEE international conference on communication, networking and broadcasting*, pp. 3759–3763.
15. Sun, Y. L., Han, Z., Yu, W., & Ray Liu, K. J. (2006). Attacks on trust valuation in distributed networks. In *Proceedings of 40th annual conference on information sciences and systems*, pp. 1461–1466.
16. Ming-Yang, S. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection system. *Computer Communications*, *34*(1), 107–117.
17. Djahel, S., Naït-abdesselam, F., & Zhang, Z. (2010). Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. *IEEE communications surveys and tutorials*, *13*(4), 658–672.
18. Agrawal P., Ghosh, R. K., & Das, S. K. (2008). Cooperative black and gray hole attacks in mobile ad hoc networks. In *Proceedings of 2nd international conference on ubiquitous information management and communication Korea*, pp. 310–314.
19. Baadachen, A., & AliBelmehdi, (2012). Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. *Journal of Network and Computer Applications*, *35*(3), 1130–1139.
20. Yu, H., Shen, Z., Miao, C., Leung, C., & Niyato, D. (2010). A survey of trust and reputation management systems in wireless communications, In *Proceedings of IEEE*, pp. 1755–1772.
21. Marti, S., Giuli, T.J., Lai, K., & Baker, M. (2000). Mitigating routing misbehaviour in mobile ad hoc networks. In *Proceedings of 6th annual international conference on mobile computing and networking*, pp. 255–265.
22. Buchegger, S., & Boudec, J. (2002). Performance Analysis of the CONFIDANT protocol: Cooperation of nodes-fairness in distributed ad hoc networks. In *Proceedings of IEEE/ACM workshop mobile ad hoc networking and computing*, pp. 226–236.
23. Michiardi, P., & Molva, R. (2002). Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of sixth joint working conference on communication and multimedia*, pp. 107–121.
24. Wang, J., Liu, Y., & Jiao, Y. (2011). Building a trusted route in mobile ad-hoc networks considering communication reliability and path length. *Journal of Network and Computer Applications*, *34*(4), 1138–1149.
25. Resnick, P., & Zeckhauser, R. (2001). Trust among strangers in internet transactions: Empirical analysis of eBays's reputation system. *The Economics of the Internet and E-commerce*, *11*, 127–157.
26. Yang, H., Shu, J., Meng, X., & Lu, S. (2006). SCAN: Self-organized network-layer security in mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications*, *24*(2), 261–273.
27. Li, X., Jia, Z., Zhang, P., Zhang, R., & Wang, H. (2010). Trust-based on-demand multipath routing in mobile ad hoc networks. *IET Information Security*, *4*(4), 212–232.
28. Marina, M.K., & Das, S.R. (2001). On-demand multipath distance vector routing in ad hoc networks. In *Proceedings of international conference for network protocols*, pp. 14–23.
29. http://www.isi.edu/nsnam/ns/. July 2009.

**U. Venkanna** obtained his degree in Computer science and Information Technology in 2005 from Kshatriya college of Engineering, J.N.T.U. Hyderabad and Post graduate degree in Software Engineering in 2009 from Rmappa Engineering College, J.N.T.U. Hyderabad, Andhra Pradesh, India. He is currently doing research in National Institute of Technology (NIT), Tiruchirappalli, Tamil Nadu, India. His research interests Trust management and Reliable routing for Ad Hoc Networks.

**Jeh Krishna Agarwal** obtained his degree in Computer Science and Engineering in 2013 from N.I.T, Tiruchirappalli, Tamil Nadu, India. He is currently working as a Software Developer and Technical Analyst at Goldman Sachs.

**R. Leela Velusamy** obtained her degree in Electronics and Communication Engineering in 1986 from REC Tiruchirappalli and Postgraduate degree in Computer science and engineering in 1989 from REC Tiruchirappalli. She was awarded Ph.D. degree by the NIT Tiruchirappalli in 2010. Since 1989, she has been in teaching profession and currently she is a Associate professor in the Department of C.S.E, N.I.T. Tiruchirpapalli, Tamil Nadu,India. Her research interests include QoS routing, Adhoc Networks, Socical Networks and Digital forensics.