Wireless Netw (2017) 23:2227–2237
DOI 10.1007/s11276-016-1284-1

Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET

Priya Sethuraman[1] · **N. Kannan**[2]

Published online: 11 May 2016

Abstract The characteristics of MANET such as decentralization, dynamic topology and openness are susceptible for security threats. To overcome the security threats and to provide a reliable network to transmit packets, a need for trust based routing arises. Moreover, the trust along with energy requirement on ad hoc on demand distance vector have paved way for the development of the newly proposed algorithm named as refined trust and energy based ad hoc on demand distance vector algorithm which is the refined form of the existing trust and energy based ad hoc on demand distance vector algorithms and the classical AODV. In this paper, the refinement parameter is the trust. Moreover, Bayesian probability is introduced in this paper for trust management due to its ability to handle uncertainty for obtaining the refined form of Trust calculation. The proposed algorithm routes the packets from the source to destination not through the shortest route but by selecting a reliable route which consumes low energy and trustful for sending the packets. The simulation results obtained from this work show that the proposed algorithm performs better than the existing algorithms in terms of Trust based routing and energy efficiency.

Keywords MANET · Trust · Energy · Security · Routing · ReTE-AODV

✉ Priya Sethuraman
priyaprabhaharan@gmail.com

[1] Anna University, Chennai, India

[2] Department of Computer Science and Engineering, Jayaram College of Engineering and Technology, Tiruchirappalli, India

1 Introduction

The need for wireless connectivity and communication came into existence with the invention of mobile devices like personal digital assistant (PDA), notebook, cell phone and laptop. Wireless connectivity is classified into two groups namely infrastructure oriented such as Wi-Fi [1], worldwide interoperability for microwave access (Wi-Max) [1] and infrastructure-less as in mobile ad-hoc networks (MANETs) [2–4]. The motivation of MANETs is from the military applications where there is no infrastructure and now MANET is the key communication technology in areas like disaster relief, sensor networks and personal area networks [4]. The challenges of MANET include the openness, nomadic and lack of centralized infrastructure. The complimentary classes that safeguard MANETs are proactive, reactive and hybrid nature with respect to routing. The proactive protocols are table driven which have the routes to any destination in the network. The key challenge lies in the control overhead in maintaining routes which may not be traversed. Examples of proactive routing protocols are destination sequenced distance vector (DSDV) routing protocol, wireless routing protocol (WRP) and optimized link state routing (OLSR) protocol. Reactive Protocol is on demand based and routes are discovered on demand as the name implies. The end to end packet delay is more in reactive protocol [5] compared to table driven protocols. Examples of reactive protocols are AODV [6], DSR and others. The hybrid protocol inherits the features of both proactive and reactive protocols. Zone routing protocol (ZRP) is the popular example of hybrid routing protocol.

Inspite of dynamic topology and openness, a reliable routing algorithm is required for effective routing in MANET. Another problem with routing protocols is the

provision of security. Among all the secure routing protocols, identity based cryptography (IBC) based routing protocol proposed by Zhao [7] is the best suited security among all cryptographic solutions for MANET. However, the security provided by cryptography based algorithms is time consuming and become easy for the attackers with the availability of powerful computers. Therefore, trust management is a new solution which can handle the security of packets sent through the network effectively. Moreover, the trust management which is proposed in this paper is capable of overcoming the security problems in MANET. It is based on the concept of assigning a trust value to each node dynamically. The key factor for the calculation of trust is the behavior of the node.

Due to the consequence of dynamic topology, the trust and energy level of every node must be incorporated with dynamic calculation. In this work, two types of trust values namely direct trust and indirect trust are calculated for each node to perform trust management. Moreover, the reliable route discovery with energy efficiency and trustworthy of nodes are considered to select a route from the source to the destination. In this work, the secured and energy efficient route is established by providing the extensions to the existing TEAODV [8]. The major contributions of this paper include: (1) new methods for dynamic calculation of direct and indirect trust values for each node and incorporating them in the route discovery process to make the route trustworthy, (2) new technique for the computation of energy values of each node which helps to establish energy effective routing, (3) proposal of a dynamic network field which access the route dynamically for identifying the malicious nodes and non cooperative nodes and to eliminate such nodes from the selected route.

The rest of the paper is governed as follows. Section 2 provides the survey of related work. Section 3 shows the trust value calculation algorithm and energy computation methods and explains the proposed ReTE-AODV algorithm which uses trust and energy. Section 4 analyses the performance and effectiveness of the proposed scheme. Finally, Sect. 5 gives conclusion and future work.

2 Literature survey

Many works are available in the literature which discuss about energy efficient and secure routing protocols [9–12]. Cano and Manzoni [13] explained the energy consumption of various routing protocols like dynamic source routing (DSR), AODV, temporally ordered routing algorithm (TORA) and DSDV based on the parameters namely routing overhead, latency and route length with respect to energy consumption. Their simulation result revealed that the DSR and AODV outperformed DSDV and TORA with respect to energy efficient routing. Xiao et al. [14] proposed a flexible quality of service model for MANET which addresses the nodes dynamic roles, hybrid provisioning and adaptive conditioning.

Sergio et al. [15] proposed a trustworthy routing model using watchdog which identifies the misbehaving nodes. They used a path rater which helps to route the packets by avoiding the misbehaving nodes. Moreover, the watchdog listens to the other nodes and records their information. Using this information, the path rater derives the value of behavior nodes. The node always rates itself as 1.0 but when the path rater identifies the nodes, it assigns a neutral value of 0.5. Negative value −1 is assigned to suspected and misbehaving nodes. The route is discovered based on the calculated values by eliminating selfish nodes and malicious nodes and in the path. The weakness of watch dog is ambiguous due to sender side collisions and receiver side collisions. COllaborative Reputation (CORE) model is designed by Michiardi and Molva [16] has also a watchdog which compliments itself by a reputation model that is differentiated as subjective reputation (nodes own observations), indirect reputation [neighbor nodes (NNs) observation] and functional reputation (monitor). The model is designed to calculate trust of a node based on the reputations.

Cooperation of nodes, fairness in dynamic ad hoc networks (CONFIDANT) proposed by Buchegger and Le Boudec [17] is the modified version of watch dog and path rater which have added modules like trust manager and a reputation system in addition to the existing ones. The responsibility of the trust manager is to evaluate the events monitored by the watchdog and proclaim alarm regarding the presence of malicious nodes. The protocol is designed to apply deviation test for packets and reject them when the node's trust value goes below the threshold value. In the model proposed by Pizarda and McDonald [18], the receiver collision problem and ambiguous collision problem are rectified by assigning weights to different trust levels. Jiang and Baras [19] proposed a swarm intelligence paradigm for trustworthy routing in MANET. In their model, routing is influenced by a certificate table (CT) wherein each entry corresponds to a certificate. Instead of calculating the hop count, the metric lies in choosing the neighbor as next hop to traverse to the destination. Their algorithm used ant-based evidence distribution and reinforcement rules which contribute to establish the optimal path that is governed by security metrics namely the network source availability and entity trustworthiness.

Panagiotis and Zygmunt [20] in their work have proposed two protocols called secure message transmission (SMT) protocol and the secure single-path (SSP) protocol which can be utilized in wide range of architectures. The protocols are capable of operating in an end to end manner. The trust of the network is calculated using these protocols.

The path is trustworthy as the protocols are efficient to detect transmission failures and can dynamically reconfigure using trusted destination feedback to avoid data loss. Trust based incentive model proposed by Wang et al. [21] has a trust scaling factor which is designed to accommodate accurate trust value by neglecting fake information. Another version of trust based incentive model was proposed by Velloso et al. [22] which adopts trust evaluation method which derives its value from trust scaling factor. This self policing mechanism is also designed to neglect fake information. Shabut et al. [23] proposed a trust model with defense scheme which filters attacks dynamically using time parameter to sieve dishonest recommendations. Pandit and Ladhe [24] proposed a trusted communication routing in MANET using a trust allocation certificate (TAC) which declares the trustworthiness of the node. In their model, network overhead is minimized as the TAC is imbibed with periodic TAC Expiration mechanisms.

Inspite of the presence of many works in the literature, the security and energy issues in MANET are not solved fully. Therefore, it is necessary to propose a new protocol which can handle these issues dynamically. Hence, we propose a refined trust and energy based ad hoc on demand distance vector algorithm (ReTE-AODV) for effective routing in MANET.

3 Trust management model

Trust management model is the methodology which enhances the routing performance in MANET. The five basic properties [25, 26] of trust in MANET are subjectivity, dynamicity, non-transitivity, asymmetry and context dependence. In this paper, a new trust management model is proposed to enhance the security of packets routed through the network. For this purpose, two trust values namely direct and indirect trust values are used. The final trust value (FTV) is derived based on direct trust value (DTV) and indirect trust value (IDTV). In this work, the Trust value of any given node in the topology holds the value between 0 and 1 i.e. $(0 \leq \text{DTV} \leq 1)$; $(0 \leq \text{IDTV} \leq 1)$. The value 0 denotes feeble trustworthiness whereas the value 1 denotes the most trustworthy nodes. The refined trust energy-ad hoc on demand distance vector ReTE-AODV algorithm proposed in this paper is the refined version of the existing TE-AODV [8] protocol. The major extensions are focused on trust management and energy optimization.

3.1 Refined trust energy-ad hoc on demand distance vector ReTE-AODV

3.1.1 Assumptions

1. All links are Bi directional.
2. The path rater initializes DTV = 0.5 for all the nodes.
3. The FTV lies in the range [0, 1]; $(0 \leq \text{FTV} \leq 1)$.
4. The entire node in the topology operates in promiscuous mode.
5. All nodes have equal energy initially.

3.1.2 Final trust value calculation

The Algorithm1_FTV_cal(node n) is used to calculate the FTV of the given node based on the values obtained from the DTV and IDTV calculation.

3.1.2.1 Direct trust value calculation Direct Trust Value of a node 'n' is determined based on the ratio of the packets received to that of the packets transmitted at a given time as assessed by its peer node. DTV computed using the Eq. 1, is incorporated in the Step 3 of Algorithm1_FTV_cal().

$$\begin{aligned} DTV_{ij}[n] = |\mu^f \times w1 \times SP_{ij}[n] + w2 \times 1 - RP_{ij}[n] + w3 \\ \times DC_{ij}[n] + w4 \times 1 - TF_{ij}[n] + w5 \times HP_{ij}[n] \\ + 1 - TF_{ij}[n] \times DTV_{ij}[n-1]| \end{aligned} \tag{1}$$

where $SP_{ij}(n)$ = no. of packets successfully sent from source i to destination j, $RP_{ij}(n)$ = received packet rate, $DC_{ij}(n)$ = data consistency, $TF_{ij}(n)$ = time frequency, $HP_{ij}(n)$ = hello packets sent and acknowledge feedback, μ^f = network field, $w_1, w_2, \ldots, w_5$ are the weights assigned.

3.1.2.2 Indirect trust value calculation IDTV of Node 'n' is determined based on the history of node n's behavior to nodes i and j. The assessments made by i, j on n can be reproduced as recommendations of a particular node at a particular time. The computation of IDTV performed using Eq. 2, is incorporated in the Step 5 of Algorithm1_FTV_cal().

$$IDTV_{ij}[n] = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} RTV_{ij^{(n)}}}{N} + \mu^f \tag{2}$$

The FTV calculation algorithm is as follows:

Algorithm1_FTV_cal(node n)

Step1 : initialize DTV = 0.5 for all the nodes // By path rater

Step2 : $\mu^{f} = \frac{S_{ij(n)}}{F_{ij(n)}} + S_{ij(n)} / [\frac{S_{ij(n-1)}}{F_{ij(n-1)}} + S_{ij(n-1)}]$ // S – packet forward success from node i to j

Step 3 : calculation of DTV(n) // F- packet forward failure from node i to j

Step 3.1 : if (node i and node j do not interact) then

$DTV_{ij}[n] = 0.5$

Step 3.2 : else

if $FTV_{ij}[n] > DTV_{ij}[n]$ then

compute DTV from the parameters SP, RP, DC, TF, HP by applying equation 1

Step 4 : if(DTV[n] ≥ 0.5)

assign α as 1 and β as 0

Step 5 : else

assign α as 0.5 and β as 0.5

compute IDTV from RTV and μ by applying equation 2

Step 6: $FTV_{ij}[n] = \alpha \times DTV_{ij}[n] + \beta \times IDTV_{ij}[n]$

3.1.2.3 Energy value calculation Energy is consumed whenever a packet is sent or received and during overhear by the NNs. Energy consumption of node n is derived using Eq. 3.

$$E_c(n) = \left[P_t \times \frac{D_s}{D_r} - P_r \times \frac{D_s}{D_r}\right] + n \times P_o \quad (3)$$

where $E_c(n)$ = energy consumed by node n, P_t = transmitting power, D_s = data size, D_r = data rate, P_r = receptive power, P_o = loss due to overhearing.

The node n's remaining energy (RE) $E_r(n)$ is calculated using Eq. 4, is incorporated in the Step 7 of Algorithm2_RREQ ().

$$E_r(n) = E_i(n) - E_c(n) \quad (4)$$

where $E_i(n)$ = initial energy, $E_c(n)$ = consumed energy.

Energy level for any node at a given time is calculated frequently and RE percentage of a particular node is derived. If the derived percentage is found to be <50, then the node will not forward any more packets and the energy level is assigned with value 0 else 1. Packets will be forwarded till the node reaches value 0. In the NN table, each node stores the information about its id, final trust value and energy level. Moreover, the NN table enables the nodes to select suitable NNs to forward packets based on the information available in NN table.

3.1.3 Route selection

The proposed algorithm ReTE-AODV is the enhanced version of TE-AODV and AODV which are reactive routing protocols which is designed to establish a trustworthy the route from source to the destination. The routing process comprises of route discovery phase and route maintenance phase.

3.1.3.1 Route discovery The objective of route discovery process is to discover a trust worthy route from source to destination. The source node initiates the route discovery by checking in the existing routing (ER) table for a secured and energy efficient route to the destination. If there exist such a route, a trusted route request (TRREQ) packet is generated by the source node and is forwarded to the intermediate nodes. The trust route (TR) value is calculated at the destination based on the total trust value and the HopCount using the formula given in Eq. 5 which is incorporated in the Step 2 of Algorithm2_RREQ ().

$$TR = \text{Final Trust/HopCount} \quad (5)$$

If the TR is greater than threshold, then the TRREQ is broadcasted in the existing route otherwise new route should be discovered. In this way, the Route Discovery comprises of three steps namely RREQ, RREP and Best route selection

as shown in the Algorithm2_RREQ(), Algorithm3_RREP(), Algorithm4_Best_route() respectively.

3.1.3.2 Route request In this work, Bayesian probability [27] approach is used to modify the existing AODV to handle the trust management issues. Here, the Bayesian probabilistic theory is intended to manipulate conditional probabilities. Moreover, the joint probability consists of two events namely hypothesis and data represented using Eq. 6.

$$P(H|D) = \frac{P(D|H) \times P(H)}{P(D)} \quad (6)$$

The intermediate node which receives RREQ message will calculate the Bayesian probability P_i using the neighborhood density D_i as in Eq. 7. It is incorporated in the Step 3 of Algorithm2_RREQ ().

$$P_i = P(D|D_i) \times P(Di)/[P(D|D_1) \times P(D_1) + P(D|D_2) \times P(D_2) + \cdots + P(D|D_n) \times P(D_n)] \times i/2(n_n/n_e) \quad (7)$$

The n_n, n_e in the equation represents number of neighbors and the minimum expected neighbors. If $P_i < r$ and $TR < THRESHHOLDVALUE$, then RREQ packets are broadcasted when then the probability falls below the random number ranges from 0 to 1 and when the TR is less than the threshold value. The steps of the route request process depicted in Algorithm2_RREQ() follows:

```
Algorithm2_RREQ ( )
Step 1 : ER is checked in Routing Table by Source Node      /* ER - Existing Route */
Step 2 : if (ER exists in routing table)
          TRREQ is generated
          calculate TR from final trust and hopcount by applying equation 5
Step 3 : if (not destination node)
          compute  Pi by applying equation 7
Step 4 :  if ( Pi< r and TR < THRESHHOLDVALUE ) then
           broadcast RREQ
Step 5 : neighbour nodes receive RREQ
Step 6 : if ( IPAddress , RREQID) exists in the routing table then
          drop RREQ
Step 7 : else
           lookup NN table for neighbours FTV and  Er(n)  calculated from equation 4
           Step 7.1 : if (FTV and Er(n)  > 0.5)
           Step 7.2 : repeat at each node in the discovered path until destination
                      Total Trust value in TRREQ = Current FTV + Next Node FTV
                      HopCounter ++
                      forward modified TRREQ  to the neighbours.
            Step 7.3 : else
                       ignore and drop RREQ.
```

3.1.3.3 Route reply The steps of the route reply process given by Algorithm_RREP() follows:

Algorithm_ RREP ( )

Step 1 : Choose first two RREP packets

Step 2 : Enter Neighbour list from the selected RREP packets

Step 3 : Collect RREP from Neighbour Nodes

Step 4 : For i=1 to n

$$NTF = \frac{\sum_{i=1}^{N} NTF_i(n)}{N}$$

Step 5 : RREP is forwarded to source node from destination node.

3.1.3.4 Best route selection All the RREP packets received by the source node are sorted using the trust values and energy levels. The first RREP is the NN selected for first hop. The route selection methodology is to select a trustworthy route rather than a shortest route. In very few cases the trustworthy route and shortest route will be the same. The steps of the best route selection algorithm enlisted in Algorithm4_Best_route() follows:

Algorithm4_Best_route( )

Step 1 : sort RREP by NTF

Step 2 : choose the first RREP

Step 3 : source node selects this node for communication

Step 4 : repeat the process till the destination is reached

3.1.3.5 Route maintenance In this work, route maintenance is based on the probability values. If the probability values are more than the threshold and the topology is not changing then the same route is maintained. Otherwise, a new route is discovered again by invoking the route discovery process. For maintaining routes, the path provided in the routing table based on the nodes traveled by the Route REPly packet (RREP) is used as the best route. Therefore, it is assumed that the RREP avoids the malicious nodes and travels only through the trusted nodes having the minimum energy. Algorithm5_RERR() depicts the procedure to overcome the error caused in the route.

Algorithm5_RERR( )

Step 1: if RERR is received then look up routing table and remove routes containing malicious nodes, broken links

Step 2: initiate new route discovery after removal of few specific nodes or route

Table 1 The environment setup for ReTE-AODV

Simulation software	QualNet 4.5
Interface IDE	Visual Studio 2013 update 3 (MBCS installed)
Programming language	Visual C++
Runtime libraries	Advanced C 8.1
SDK	QNSDK
Simulation area	5 sq. km
Node RF range	1500 m
Node RF Strength	27 dbm @ 500 mW
Node power source	1500 mAh standard Li-ion battery
Number of simultaneous nodes	100
Simulation time	300 s
Node mobility	Random
Data packet size	4096 B (4 kB)
Maximum speed	25 ms
Traffic type	Constant bit rating

4 Simulation and result analysis

In this section, the effectiveness of the proposed algorithm refined trust energy-ad hoc on demand distance vector ReTE-AODV is provided using the simulation results generated by the simulator QualNet 4.5 [28].

4.1 Environment settings

The environment set up used to carry out the simulation is shown in Table 1.

4.2 Performance parameters

Performance is evaluated using three different scenarios and six different metrics. The performance metrics considered for simulation is as follows:

1. *Packet delivery ratio (%)* It is the ratio of the packets received by destination node to that of the packets sent by the source node.
2. *Average end to end latency (ms)* The average time taken by the packets to reach the destination node which includes transmission delay, propagation delay, processing delay, queuing delay.

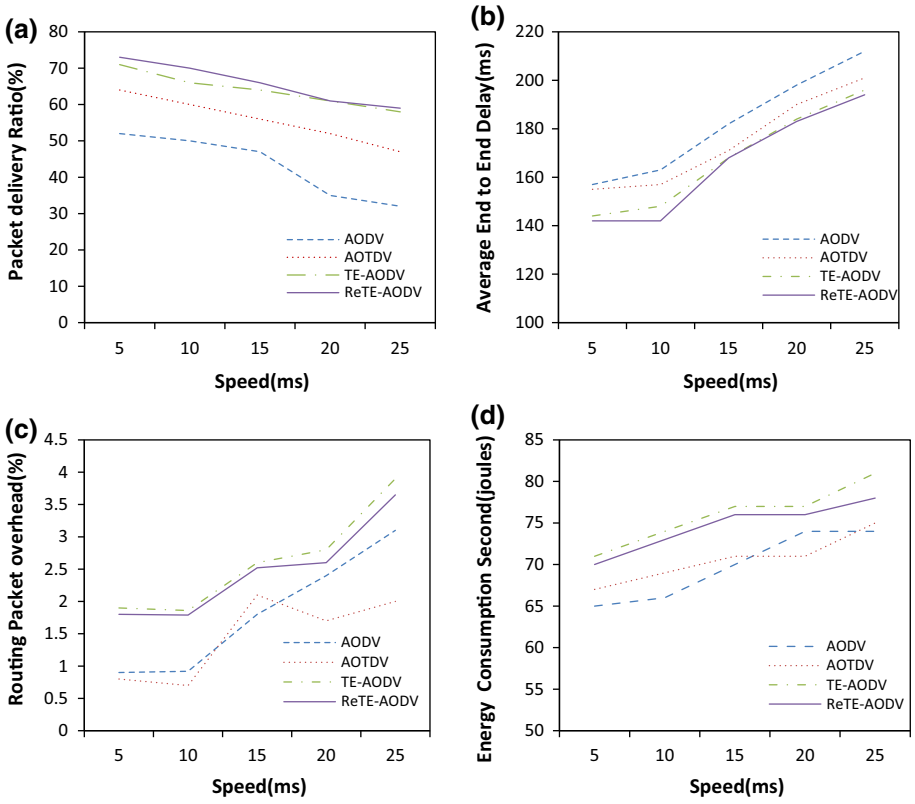

Fig. 1 Varying node velocity. **a** Packet delivery ratio analysis, **b** average end to end delay analysis, **c** routing packets overhead analysis and **d** energy consumption analysis

3. *Routing packet overhead (%)* It is the ratio of the control packets generated to that of total number of data packets sent.
4. *Energy consumption (Joules)* Energy consumption of the nodes per second.

4.3 Result analysis

The performance of the proposed algorithm ReTE-AODV was observed for three different scenarios [8]. Scenario 1 is the Node velocity. It is varied from 5 to 25 m/s in step of 5 m/s. Scenario 2 simulation result is observed by varying the number of malicious nodes ranging from 0 to 20 in step of 5. Scenario 3 simulation study is performed by varying the threshold values from 0.02 to 1 in steps of 0.02. The above mentioned simulation scenarios are discussed using the performance of the proposed algorithm ReTE-AODV with TE-AODV, AOTDV and AODV.

4.3.1 Scenario 1: varying node velocity

In the scenario1, the node velocity is varied from 5 to 25 ms in steps of 5 ms. The parameters considered for evaluating the performance of the proposed algorithm are packet delivery ratio percentage, average end to end delay in milliseconds, routing packet overhead (RPO) percentage and energy consumption per second in joules. The observed values are plotted as graph in Fig. 1.

Figure 1(a) depicts the graph of node velocity versus packet delivery ratio% for the AODV, AOTDV, TE-AODV and the proposed ReTE-AODV routing algorithms. It is visible from the graph that ReTE-AODV performs better than the other algorithms and the better performance is obtained when the node velocity is between 10 and 15. The TE-AODV and ReTE-AODV have almost the same values when the node velocity is between 20 and 25. This is because both the algorithm selects the NN based on FTV value and RE and the proposed algorithm is the refined form of TE-AODV. The packet delivery ratio obtained by the proposed algorithm is high due to the methodology followed in the algorithm implementation for the intermediate node selection. The parameters which boost up the packet delivery ratio such as elimination of malicious and selfish nodes and very feasible packet drop in intermediate nodes are well ascertained while designing the proposed algorithm. Energy is considered while establishing connections only in algorithm TE-AODV and ReTE-AODV whereas AODV and AOTDV do not consider energy as a parameter for establishing path and hence the latter algorithm results low in packet delivery ratio.

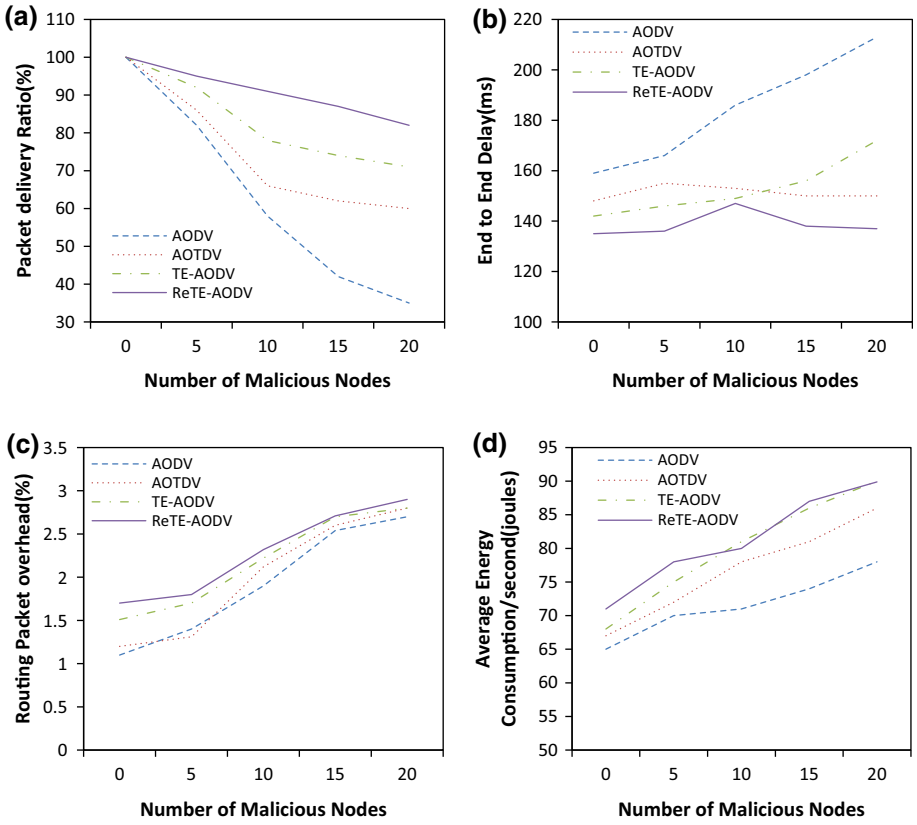

Fig. 2 **a** Packet delivery ratio analysis, **b** average end to end delay analysis, **c** routing packets overhead analysis and **d** energy consumption analysis

Figure 1(b) depicts the graph of for node velocity versus average end to end delay. It is obvious that the average end to end delay increases with increase in the node velocity. Classical AODV algorithm do not use trust whereas AOTDV, TE-AODV and the proposed ReTE-AODV are trust based algorithm designed to perform better by eliminating the malicious and selfish nodes in the route and to reduce the average end to end delay.

Figure 1(c) depicts the graph of node velocity versus RPO. The plotted values ensures that the proposed algorithm have lesser RPO compared to the TE-AODV. The reason behind this is the algorithm is designed to achieve good results and optimized for transfer of control packets without elevating the RPO. The ReTE-AODV has higher RPO compared to AODV, AOTDV as these algorithms have minimal exchange of control packets which makes these algorithms less trustworthy.

Figure 1(d) depicts the graph of node velocity versus energy consumption per second in joules. The values of the TE-AODV and ReTE_AODV are higher compared to the other algorithms as energy consumed is high while traversing the data and control packets of the trust algorithms. Energy consumption is increased with increase in the node velocity.

4.3.2 Scenario 2: varying the number of malicious nodes

In the Scenario 2, the simulation is performed by varying the number of malicious nodes ranging from 0 to 20 in steps of 5 on the parameters like packet delivery ratio percentage, average end to end delay in milliseconds, RPO percentage and energy consumption per second in joules. The observed values are plotted as graph in Fig. 2.

Figure 2(a) depicts the graph for varying number of malicious nodes versus packet delivery ratio for the AODV, AOTDV, TE-AODV and the proposed ReTE-AODV routing algorithms. It is visible from the graph that ReTE-AODV performs better than the other algorithms. This is because the proposed algorithm selects the NN based on FTV value and RE and since this calculation is dynamic the behavioral patterns of the node is reflected immediately in the direct trust value calculation and indirect Trust value calculation which inturn is reflected in the FTV value. The parameters which boost up the packet delivery ratio such as elimination of malicious and selfish nodes, very feasible packet drop in intermediate nodes are well ascertained while designing our proposed algorithm. Energy is considered while establishing connections only in algorithm TE-AODV and ReTE-AODV

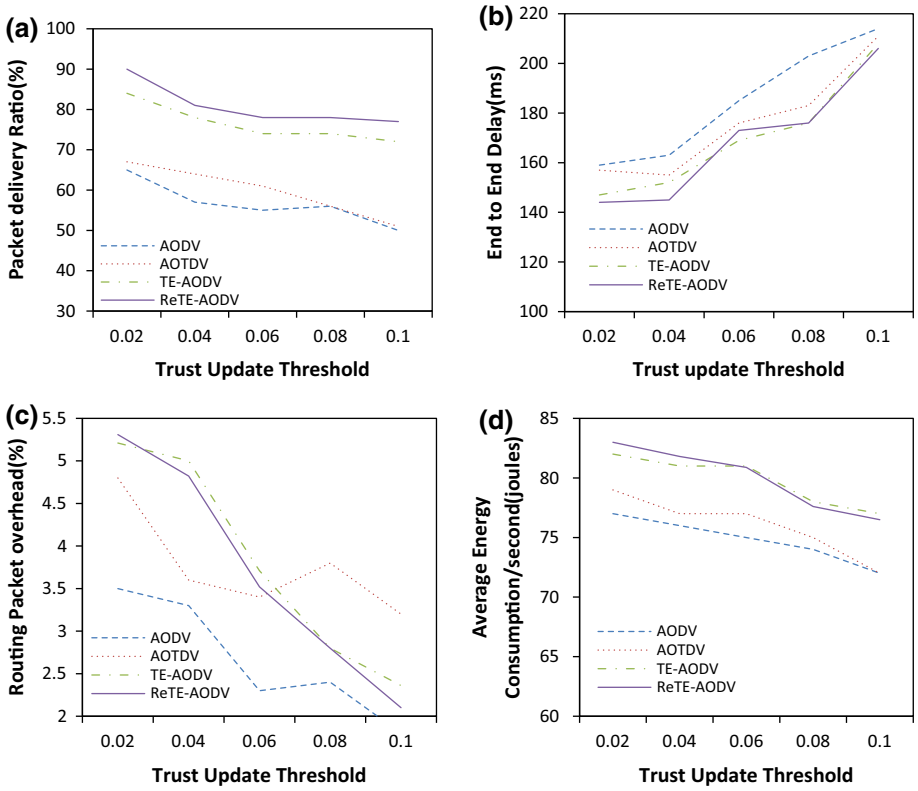

Fig. 3 Varying trust update threshold. **a** Packet delivery ratio analysis, **b** average end to end delay analysis, **c** routing packets overhead analysis and **d** energy consumption analysis

whereas AODV and AOTDV do not consider energy as a parameter for establishing path and hence the latter algorithm results low in packet delivery ratio.

Figure 2(b) depicts the graph for varying number of malicious nodes versus Average end to end delay. It is obvious that the average end to end delay of the classical AODV algorithm is high. This is because the NNs chosen from AODV algorithm has many malicious nodes in it whereas the proposed ReTE-AODV algorithm is designed to eliminate choosing malicious node and selfish node in its path and hence the end to end delay is feasible.

Figure 2(c) depicts the graph for varying number of malicious nodes versus RPO. The control packets and data packets are sent in the network. Even though TRREQ and trusted RREPs are broadcasted in the network the RPO is less in the proposed algorithm compared to TE-AODV.

Figure 2(d) depicts the graph of for varying number of malicious nodes versus energy consumption per second in joules. The Energy consumption of the proposed algorithm is little high due to the extensive computation involved in tracking and eliminating the malicious and selfish nodes in the path and thus establishes a trust worthy path for transmission of packets.

4.3.3 Scenario 3: varying trust update threshold

Scenario 3, the simulation study is performed by varying the threshold value from 0.02 to 1 in steps of 0.02 on the parameters like Packet delivery ratio percentage, Average end to end delay in milliseconds, RPO percentage and Energy consumption per second in joules. The Observed values are plotted as graph in Fig. 3.

Figure 3(a) depicts the graph of varying trust update threshold versus packet delivery ratio for the algorithms AODV, AOTDV, TE-AODV and the proposed ReTE-AODV. It is obvious from the graph that the proposed algorithm outperforms all the other algorithms in the packet delivery ratio which is considered as a vital parameter in accessing the quality of the network. The Trust Update Threshold value is ensured to be greater than the trusted route and the Bayesian probability computation value should be less than the random value [i.e. If ($P_i < r$ and $TR < THRESHHOLDVALUE$)] to broadcast a packet. These methodologies imbibed in the algorithm make the algorithm effectively delivery packets compared with other algorithms.

Figure 3(b) depicts the graph of varying trust update threshold versus average end to end delay. The algorithm ReTE-AODV gets better results compared to the other three algorithms. However, when the trust update threshold

is between 0.05 and 0.06 TE-AODV has lower delay than the proposed algorithm in this simulation run. But the ReTE-AODV outperforms in the average run.

Figure 3(c) depicts the graph of varying trust update threshold versus RPO. The RPO is minimized with the increase in the trust update threshold value. The overhead is more in the proposed algorithm due to the number of control packets flooded in the network.

Figure 3(d) depicts the graph of varying trust update threshold versus energy consumption per second in joules. Energy consumption is high in ReTE-AODV. Even though energy consumption is high, the trustworthiness of the route is not compromised and thus making the proposed algorithm more reliable.

5 Conclusion and future work

In this paper, a Refined Trust based Energy effective routing algorithm ReTE-AODV is proposed and compared with AODV, AOTDV, TE-AODV and evaluated under three simulation scenarios. From the experiments conducted in this work, it is observed that the proposed algorithm ReTE-AODV outperforms the other three existing algorithms. In the proposed model, in spite of having high values in RPO and energy consumption due to the extensive computation of FTV value dynamically, the throughput of the algorithm is not compromised. The results reveal that the proposed algorithm performs better than the other three algorithms with respect to packet delivery ratio and average end to end latency. Moreover, the proposed algorithm provides a trustworthy route for MANET inspite of its dynamic topology and openness.

Many future works are possible in this area. It is possible to use intelligent rules to make effective decisions in routing. Intelligent Agents can be deployed at each sensor node which can vary the transmission rate to avoid congestion at base station. Finally, particle swarm optimization technique and reinforcement learning can be used to perform overall optimization with respect to routing decisions.

References

1. Murthy, C. S. R., & Manoj, B. S. (2004). *Ad hoc wireless networks: Architectures and protocols, portable documents*. New Jersey: Prentice Hall.
2. Chlamtac, I., Conti, M., & Liu, J. J. N. (2003). Mobile ad hoc networking: Imperatives and challenges. *Ad Hoc Networks, 1*(1), 13–64.
3. Perkins, C. E. (2001). Ad hoc networking: An introduction. *Ad Hoc Networking, 40*, 20–22.
4. She, C., Yi, P., Wang, J., & Yang, H. (2013). Intrusion detection for black hole and gray hole in MANETs. *TIIS, 7*(7), 1721–1736.
5. Zuhairi, M., Zafar, H., & Harle, D. (2012). Dynamic reverse route for on-demand routing protocol in MANET. *KSII Transactions on Internet and Information Systems (TIIS), 6*(5), 1354–1372.
6. Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (No. RFC 3561). Internet Society.
7. Zhao, S., Aggarwal, A., Frost, R., & Bai, X. (2012). A survey of applications of identity-based cryptography in mobile ad-hoc networks. *IEEE Communications Surveys & Tutorials, 14*(2), 380–400.
8. Venkanna, U., Agarwal, J. K., & Velusamy, R. L. (2015). A cooperative routing for MANET based on distributed trust and energy management. *Wireless Personal Communications, 81*(3), 961–979.
9. Kulothungan, K., Ganapathy, S., Indra Gandhi, S., & Yogesh, P. (2011). Intelligent secured fault tolerant routing in wireless sensor networks using clustering approach. *International Journal of Soft Computing, 6*(5), 210–215.
10. Balachandra, M., Prema, K. V., & Makkithaya, K. (2014). Multiconstrained and multipath QoS aware routing protocol for MANETs. *Wireless Networks, 20*(8), 2395–2408.
11. Xia, H., Yu, J., Pan, Z. K., Cheng, X. G., & Sha, E. H.-M. (2015). Applying trust enhancements to reactive routing protocols in mobile ad hoc networks. *Wireless Networks*. doi:10.1007/s11276-015-1094-x.
12. Logambigai, R., & Kannan, A. (2016). Fuzzy logic based unequal clustering for wireless sensor networks. *Wireless Networks, 22*, 945–957.
13. Cano, J. C., & Manzoni, P. (2000). A performance comparison of energy consumption for mobile ad hoc network routing protocols. In *Proceedings of the 8th international symposium on modeling, analysis and simulation of computer and telecommunication systems, 2000* (pp. 57–64). IEEE.
14. Xiao, H., Seah, W. K., Lo, A., & Chua, K. C. (2000). A flexible quality of service model for mobile ad-hoc networks. In *Proceedings of the IEEE 51st vehicular technology conference (VTC 2000)-Spring Tokyo* (Vol. 1, pp. 445–449). IEEE.
15. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on mobile computing and networking* (pp. 255–265). ACM.
16. Michiardi, P., & Molva, R. (2002). Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In B. Jerman-Blažič & T. Klobučar (Eds.), *Advanced communications and multimedia security* (pp. 107–121). New York: Springer.
17. Buchegger, S., & Le Boudec, J. Y. (2004). A robust reputation system for peer-to-peer and mobile ad-hoc networks. In *P2PEcon 2004* (No. LCA-CONF-2004-009).
18. Pirzada, A. A., & McDonald, C. (2004). Establishing trust in pure ad-hoc networks. In *Proceedings of the 27th Australasian conference on computer science* (Vol. 26, pp. 47–54). Australian Computer Society.
19. Jiang, T., & Baras, J. S. (2004). Ant-based adaptive trust evidence distribution in MANET. In *Proceedings of the 24th international conference on distributed computing systems workshops* (pp. 588–593). IEEE.
20. Papadimitratos, P., & Haas, Z. J. (2006). Secure data communication in mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications, 24*(2), 343–356.
21. Wang, K., Wu, M., & Shen, S. (2008). A trust evaluation method for node cooperation in mobile ad hoc networks. In *Fifth international conference on information technology: New generations (ITNG 2008)* (pp. 1000–1005). IEEE.
22. Velloso, P. B., Laufer, R. P., Laufer, R. P., de O Cunha, D., Duarte, O. C., & Pujolle, G. (2010). Trust management in mobile

ad hoc networks using a scalable maturity-based model. *IEEE Transactions on Network and Service Management, 7*(3), 172–185.
23. Shabut, A. M., Dahal, K. P., Bista, S. K., & Awan, I. U. (2015). Recommendation based trust model with an effective defence scheme for MANETs. *IEEE Transactions on Mobile Computing, 14*(10), 2101–2115.
24. Pandit, C. M., & Ladhe, S. A. (2014). Secure routing protocol in MANET using TAC. In *First international conference on networks & soft computing (ICNSC)* (pp. 107–112). IEEE.
25. Wei, Z., Tang, H., Yu, F. R., Wang, M., & Mason, P. (2014). Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. *IEEE Transactions on Vehicular Technology, 63*(9), 4647–4658.
26. Cho, J. H., Swami, A., & Chen, I. R. (2011). A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials, 13*(4), 562–583.
27. Kanakaris, V., Ndzi, D. L., Ovaliadis, K., & Yang, Y. (2012). A new RREQ message forwarding technique based on Bayesian probability theory. *EURASIP Journal on Wireless Communications and Networking, 2012*(1), 1–12.
28. Scalable Network Technologies. (2008). http://web.scalable-networks.com/content/qualnet (Accessed May 27, 2009). Internet Society.

Priya Sethuraman is a research scholar of Anna University having more than 10 years of teaching and research experience. Her areas of interest include network security, mobile computing, parallel computing and deep learning.

Dr. N. Kannan is having 21 years experience in teaching with extensive knowledge in the area of networking and image processing, currently working as Principal, Jayaram College of Engineering and Technology, Tiruchirappalli, India.