Songklanakarin J. Sci. Technol.
42 (4), 889-896, Jul. - Aug. 2020

http://www.sjst.psu.ac.th

Original Article

Resource-based routing protocol for Mobile Adhoc Networks

Prasannavenkatesan Theerthagiri[1*] and Menakadevi T[2]

[1] *Department of Computer Science and Engineering, GITAM University, Bengaluru, India*

[2] *Adhiyamaan College of Engineering, Hosur, India*

Received: 15 February 2017; Revised: 25 October 2018; Accepted: 23 May 2019

Abstract

Mobile Adhoc Networks (MANETs) provide special extemporary applications and services in a shorter time at anytime and anywhere. In MANETs, nodes require well-organized cooperation among neighboring nodes for routing and other network operations. The non-cooperative behavior of a mobile node causes a critical problem for routing and networking. The non-cooperativeness is due to its resource-constraints like battery power, non-centralized nodes, or malicious nodes. Only cooperative nodes of the network can provide an effective routing path. To discover the cooperative nodes the present work develops the trust and energy based ad hoc on demand distance vector (TE-AODV) routing. The trust value of intermediate nodes facilitates the sophisticated cooperation. TE-AODV routing gives better results for residual energy, throughput, and routing overhead (RO) than existing routing protocols. TE-AODV routing improves the remaining energy by 5–8%, reduces RO by 8–10%, and performs 4–8% faster than other protocols on detecting non-cooperative nodes.

Keywords: MANETs, cooperation, energy/trust, resource-based routing, TE-AODV

1. Introduction

The MANET has numerous applications because it does not require any fixed infrastructure and it instantly establishes communication among wireless nodes (Marti, Giuli, Lai, & Baker, 2000). The nodes also act as host, router, as well as a transceiver. The characteristics of information are much important for the communication system/network. The nodes in MANETs can communicate directly with other nodes whenever they are within their transmission coverage area. Otherwise, the nodes should depend on other neighboring cooperative nodes to establish the communication. Likewise, an intermediate neighboring node forms communication among other mobile nodes in MANETs for routing (Rohini & Dhanasekar, 2014). Since the cooperative device (nodes) accomplishes the exact delivery of the information without any disruption, the cooperation depends on exact packet-delivery, information quality, availability, and sharing. Thus, cooperation is the required operation by every node in the network to establish any form of communication among wireless devices, especially in MANETs (Prasannavenkatesan, Raja, & Ganeshkumar, 2014).

Certain nodes behave selfishly to conserve its resources. Such nodes do not participate in the packet relaying/forwarding process and other network operations with intermediate neighboring nodes and they disturb communication among nodes and degrade network performance as well (Shakshuki, Kang, & Sheltami, 2013). A non-cooperative node drops the packet or forwards the packet either partially or incompletely to preserve battery-power, energy, bandwidth, channel, and its own resources. These nodes are also called resource-constrained nodes. Since it is quite necessary to exclude resource-constrained nodes to facilitate effective communication and routing between nodes (Prasanna venkatesan, Rajakumar, & Pitchaikkannu, 2014a), the present work concentrates on this development. Many researchers devoted their work to developing efficient network routing protocols (Chang, Tsou, Woungang, & Lai, 2015). Most of the existing research concentrates on optimizing routing protocol using trust-value and attack detection/prevention methods.

The objective of this research was to identify and exclude resource-constrained nodes and improve cooperative

*Corresponding author
Email address: prasannait91@gmail.com

communication in a MANET. Hence, this work proposes a resource-optimized routing protocol for cooperative communication among nodes. It utilizes both trust and energy values to evaluate the cooperativeness of the node. The remainder of the work is organized as follows. Section 2 discusses the recent development of routing protocols for ad hoc networks, feasible solutions for communication problems in cooperative communication establishment, and their limitations/difficulties in a MANET. It discusses various issues with the resource-constraints energy and bandwidth. Section 3 presents the development of resource-constrained routing protocol and algorithm/techniques to enhance the cooperation of the mobile node. Section 4 evaluates the present work with different scenarios and various performance metrics and compares and analyzes the existing research with the performance results of the present work. Finally, section 5 concludes the paper with future enhancements of this work.

2. Related Research

Several research studies have concentrated on optimizing network performances by enhancing the routing process. This section discusses various research reports on the development of energy/trust based routing protocol, trust/ reputation mechanisms, its advantages/restrictions, and cooperation problems in a MANET. Moreover, this section analyses the performances of different algorithms with several parameters for stimulating cooperation of the nodes. Chong, Tan, and Ng (2003) proposed Separation of Detection Authority to detect selfish nodes and improve trustiness of the nodes in the network. The nodes improve its trustworthiness using three components, namely reporting node, agent node, and central authority. Reporting node identifies the misbehaving non-cooperative node and generates reports to a central authority. Central authority investigates the reports using agent nodes. Agent nodes are the neighboring monitoring nodes. Finally, all agents submit reports concerning suspiciousness to the central authority. However, these three entities consume more energy to process the reports. The communication overload is very tight for the three entities and reduces the network performance. The proposed work considers the unavoidable energy metric and trust values of the node for routing and evaluation of distributed cooperation behavior.

Ferraz, Velloso, and Duarte (2014) presented Trust-based Exclusion Access-control Mechanism (TEAM) to compute the trustworthiness of the node using the local module and global module. Each node observes and gathers one-hop neighbors behaviors and other data in the local module. The global module receives the forwarded behavioral information and evaluates the evidence of trust using the voting mechanism. Thus, it denies access of the non-cooperative nodes to the network. The advantage of this mechanism is that it uses fewer messages for detecting and excluding misbehaving nodes. Because of the mobility nature of MANETs, it should evaluate the false positive/negative analysis for trustworthiness since it always depends on the neighboring node report. Moreover, it should strengthen the module features and friendship mechanisms with security aspects. This work does not consider the inevitable energy consumption parameter of the nodes.

Anderegg and Eidenbenz (2003) were introduced to the Ad Hoc-VCG routing protocol by Vickrey, Clarke, and Groves. In this method, each node publishes its available energy in the route discovery process. The source node (SN) chooses the cost-effective path and assigns credit to the intermediate nodes for routing. However, it is not sure that each node gives genuine energy values. It is very essential to assess the gathered values since a collision between similar energy valued nodes is likely to occur. The proposed work used trust function to overcome these limitations. Pradeep and Soumya (2011) adopted an artificial neural network (ANN) and a feed forward and back propagation algorithm to provide secure multicast routing in MANETs. A special node called ‘support node’ was introduced solely to assist the routing discovery process. The support nodes are always connected with other nodes and it gives improved performance over security and quality of service metrics. However, this paper only analyzed the theoretical work since it did not experimentally evaluate by simulation/implementation. To enhance the performance of Dynamic Source Routing protocol Gargi, Chaba, and Patel (2012) developed an ANN-based algorithm. It detects intrusions by taking routing data as input to ANN training in a MANET. The ANN tunes input values to get optimal target output. It divides the tuning dataset into training, validation, and testing datasets. It does not address complete simulation parameters and performance analysis of ANN. Moreover, it does not compare the proposed results with other work.

Zarei and Faez (2012) presented the Modified Reverse AODV (MRAODV) algorithm for a MANET to discover the best routes. It adopted the Recurrent Neural Network (RNN) based protocol to find the optimal routing path and it modified the actual Route Request (RREQ) packet into Reverse Route Request (R-RREQ). The RNN periodically monitors the fitness of routes in a MANET. The weights of nodes are computed and then fed into the feedback learning algorithm for effective routing. The effects of battery power are undefined in this work. It plays an important role in discovering the reliable routing path. Nevertheless, it analyzes fewer scenarios of performance results with a smaller simulation environment and lacks in comparison of results with other relevant work.

Extract of the literature:

1) Several research studies incorporated the reputation/credit mechanism for effective route discovery process, but many of them did not consider the unavoidable energy of the node in MANETs.
2) Recent research adopted ANN to facilitate an efficient routing path. However, these studies lacked false positive and false negative analyses.
3) To the best of our knowledge, no work has focused on energy trust metrics, and false positive/negative analyses for resource optimized routing in MANETs. The present work incorporates all of the mentioned methods/metrics.

3. Methodology

This section discusses proposed methods and techniques for optimized routing using the TE-AODV protocol, trust function/calculations, and false positive/negative functions.

3.1 Sophisticated cooperation using the TE-AODV protocol

The current work discovers resource-constrained nodes using the trust value given by neighboring nodes to examine node activities. Neighboring nodes observe the behaviors of other nodes and their cooperation among other nodes (Mohanapriya & Krishnamurthi, 2014; Prasannavenkatesan, Udhayakumar, & Ramkumar, 2014). The proposed sophisticated cooperation is established using a trust function along with trustiness information of a node given in the mathematical derivations. The trustiness calculation is supported periodically by exchanged updates between neighboring nodes. Packets dropped due to low energy of the node and packets dropped due to a collision between nodes are investigated for calculation of the trustiness. The trustiness identifies the suspicious, non-cooperative nodes and examines again for an accurate detection of non-cooperation. The TE-AODV protocol updates suspicious non-cooperating nodes on each node's neighbor list. Accordingly, it excludes the suspected nodes for a future route-discovery process. TE-AODV works by route discovery and route maintenance processes (Alkhamisi, & Buhari, 2016; Prasannavenkatesan & Menakadevi, 2016; Samian, Zukarnain, Seah, & Hanapi, 2015). Thus, it provides high-level optimal connectivity between mobile nodes. The TE-AODV routing protocol works by two modules, namely 1) trust function module and 2) false positive/negative calculation module.

3.2 Trust function

Some nodes in the MANETs do not forward the packets that they receive from other nodes to save battery power/energy as well as to survive for a longer time in the network. It degrades the packet delivery ratio (PDR) of the network. This work assumes that few non-cooperating nodes are present in the network. The TE-AODV algorithm uses the node-status and neighbor-list to invoke the trust function. The trust function gathers trust values and other observations concerning non-cooperativeness from neighboring nodes of the suspected mobile node. Trust value plays a crucial role in the detection of resource-constrained nodes in the network. Trust value can be positive or negative based on the observations of the neighboring node. Because of the mobility of nodes, each neighboring node has a different status with other nodes at different instances in the network.

On mobility, a few nodes are out of coverage for other nodes in the network. In such a period the trust value becomes negative (Fredric *et al.,* 2009; Orallo, *et al.,* 2015). While routing, the collision of packets between nodes causes faulty trustiness. It calculates the trust value of the node by an estimation of data packet dropped due to 1) energy of the node and 2) collision of the node. The following mathematical derivation determines the trustiness value of a node. Let's consider,

$PD_E \rightarrow Packets\ dropped\ due\ to\ energy\ of\ a\ node$

$PD_C \rightarrow Packets\ dropped\ due\ to\ collision\ of\ packets\ between\ nodes$

$n \rightarrow Number\ of\ sessions$

$$PD_E = k_e \times PD_E(S) + (1 - k_e) \times PD_E\,(S-1) + \cdots + (n - k_e) \times PD_E\,(S - n)$$

$$i.e. \qquad PD_E = \sum_{i=0}^{n} (i - k_e) \times PD_E(S - i) \qquad (1)$$

$$Where\ k_e = \frac{Minumum\ energy\ required\ to\ transmit}{Number\ of\ nodes\ involed\ in\ routing}$$

$$S - i = Energy\ loss\ in\ previous\ 'n'\ consecutive\ sessions$$

$$PD_C = k_c \times PD_C(P) + (1 - k_c) \times PD_C\,(P-1) + (2 - k_c) \times PD_C\,(P-2)$$

$$i.e. \qquad PD_C = \sum_{i=0}^{2} (i - k_c) \times PD_C(p - i) \qquad (2)$$

$$P - i = Packet\ loss\ in\ previous\ 'n'\ consecutive\ sessions$$

$$Where\ k_c = \frac{Number\ of\ packet\ lost}{Number\ of\ collisions}$$

Here, the session is the successful packet transmission scenario. Similarly, 'n' represents the consecutive 'n' successful packet transmission scenario. The previous sessions $S - i$ and $P - i$ are identified by using previous transmission history and routing table/history. This evaluation is conducted for each node in the routing path. The variables PD_E and PD_C in Equations 1 and 2 give packets dropped due to energy drop of a node and collision among the packets of nodes, respectively. These derivatives give the trustiness of nodes.

3.3 False positive and false negative detection (FPND)

Based on the trustiness, it updates the suspicious non-cooperative mobile nodes to the node's neighbor list. It is essential to avoid such suspicious mobile nodes from the network for routing and other operations (Chang *et al.*, 2015; Prasannavenkatesan, Rajakumar, & Pitchaikkannu, 2014). It results in the exclusion of resource-constrained nodes and formation/establishment of a reliable cooperative routing path for effective communication using the TE-AODV protocol. The false positive/negative analysis simplifies the detection of non-cooperative nodes as well as cooperative nodes in the network. The FPND of dropped packets due to energy drop of a node and a collision of packets can be estimated using Equations 3 and 4.

$$Energy_{FPND} = \frac{PD_E}{NC} * z \qquad (3)$$

$$Collision_{FPND} = \frac{PD_C}{NC} * z \qquad (4)$$

where *NC* is the number of non-cooperative nodes detected and *z* is the total number of nodes in the network.

Equations 3 and 4 give the calculations of false positive/negative detection of nodes among the non-cooperative nodes in the network. Let's consider the MANETs shown in Figure 1 as an illustration of complete cooperative routing among nodes. In this scenario, SN desires to send a packet to destination node (DN). It is required to route through cooperative intermediate nodes using the TE-AODV algorithm. The flow diagram shown in Figure 2 illustrates the workflow of the TE-AODV algorithm in MANETs with two modules, namely the trust function module and FPND module. First, the SN observes the activities of the neighboring nodes using the AODV algorithm. Then, it determines the cooperation values of the neighboring nodes using the TE-AODV algorithm. The TE-AODV algorithm invokes trust function and PD_E and PD_C calculations. The trust function module determines suspicious nodes using Equations 1 and 2 and then forwards the reports to the FPND module. The FPND module evaluates node activities using Equations 3 and 4. Subsequently, the TE-AODV algorithm discovers reliable cooperative nodes for routing.

In this current work, let's consider the threshold value as 60 for FPND because at this value, the proposed TE-AODV protocol gives better results than other existing protocols. According to the proposed FPND module, a lower threshold value produces trusted cooperative nodes. If the FPND value is above 60, then the node is considered as an untrusted and non-cooperative node since its energy level is lower than the average value or the chances of a collision are high. Therefore, the FPND module redirects to an alternative node discovery process such that the TE-AODV algorithm excludes non-cooperative nodes from the network using a suspicious list. In Figure 1, SN observes its neighboring nodes as 1, 4, and then 2, 5 to route towards DN using the TE-AODV algorithm. The trust function module evaluates the node activities and reports to the FPND module. $Energy_{FPND}$ and $Collision_{FPND}$ estimate and report that node (4) ($Energy_{FPND}$=45.5) and node (5) ($Energy_{FPND}$=33.9) are trusted, reliable cooperative nodes for DN rather than other nodes. Therefore, the routing path SN-4-5-DN is successfully discovered using the TE-AODV algorithm.

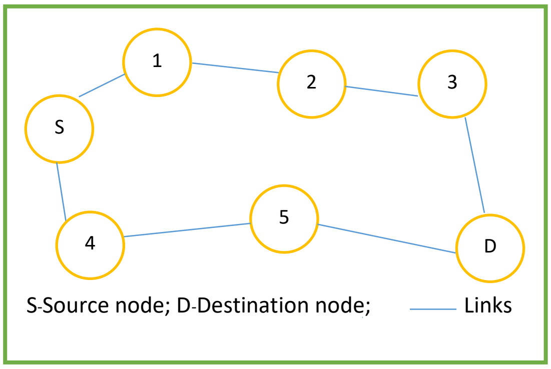

Figure 1. Co-operative packet relaying among mobile nodes.

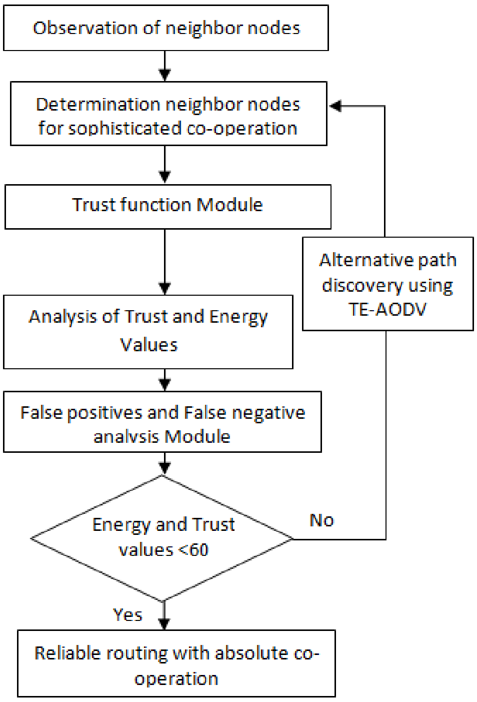
Observation of neighbor nodes
Determination neighbor nodes for sophisticated co-operation
Trust function Module
Alternative path discovery using TE-AODV
Analysis of Trust and Energy Values
False positives and False negative analysis Module
Energy and Trust values <60
No
Yes
Reliable routing with absolute co-operation

Figure 2. Flow diagram of the TE-AODV algorithm.

4. Simulation and Performance Analysis

This section summarizes the simulation of the proposed TE-AODV routing protocol and trustiness evaluation for resource optimized routing in MANETs.

4.1 Simulation environment

The Ns2 simulator (Ns2 simulator, 2016) configures the MANET to implement and evaluate the proposed approach. MANETs do not require any pre-existing infrastructure; therefore, the development of the TE-AODV routing protocol is easy to implement. The conventional AODV modifies the header to add a new field called *'slist'* to the packet header. The packet header contains the list of suspicious nodes in the network. The *slist* updates false positive/negative evaluations on each node. The packet header is modified to adopt the fields of the TE-AODV protocol. Similarly, the new header format defines the access methods, offsets, and member functions using C++ script. The *'ns-packet.tcl'* file of Ns2 incorporates all modifications and extensions of the TE-AODV protocol. It imports only the AODV header file for routing, such that it reduces the control packet overhead of the network.

The random waypoint (RWP) model directs mobility to the nodes. In RWP, each node starts moving randomly towards the destination waypoint within the specified speed limit. After that, it pauses for some time and then repeats the same until the end of simulation time. The RWP generated by the mobility scenario generation and analysis tool, namely the BonnMotion model (BonnMotion Tool, 2016). This work analyzes the performance of the TE-AODV algorithm at various sampling intervals (20, 40, 60, 80, and 100 sec**)** and different node densities (20, 40, 60, 80, and 100 nodes). It discovers the cooperative nodes at different scenarios to provide reliable routing. Table 1 summarizes the simulation parameters considered for the experiments. The simulation time is 100 sec. Mobility speed (0–10 m/s) is the speed at which the node moves in the network. Pause time is the time interval between node movements. The packet size of the constant bit rate traffic is 128–1024 bytes. The data rate is two Mbps. It configures ten (10) pairs of source and destination nodes for the simulation experiments. Table 2 illustrates the energy model parameters and values of this work. This work configures all values in the Ns2 simulation script.

4.2 Performance metrics

The following performance metrics evaluate the TE-AODV protocol with different scenarios.

4.2.1 Energy

Whenever the node broadcasts a packet, the proposed work computes the incurred energy for both transmission and reception**.** Transmission/reception power multiplies with the packet-size for computation of energy**.** Equations 5 and 6 give the energy required in joules to transmit/receive the packets**.**

$$TransmitEnergy\ (Tx) = Transmitted\ Power \times Packet\ Size \quad (5)$$

$$ReceiveingEnergy\ (Rx) = Receiveing\ Power \times Packet\ Size \quad (6)$$

4.2.2 Packet delivery ratio (PDR)

The PDR is the percentage of the packets received by the nodes to the percentage of generated packets by the SN. Equation 7 calculates the PDR.

$$PDR = \frac{Received\ packets}{Transmitted\ packets} \quad (7)$$

4.2.3 Routing overhead (RO)

Control packets used in the routing causes routing overhead. The major control packets are RREQ, route reply, and route error. The proposed work compares and analyses the incurred RO with the TE-AODV results and other protocols.

4.3 Simulation results and performance evaluation

Several scenarios evaluate the implementation results of the TE-AODV routing protocol to analyze its performance. The proposed TE-AODV protocol compares MRAODV and TEAM routing protocols with the performance metrics, namely throughput, delay, and routing overhead. It evaluates over different node densities and pause times.

Figure 3 illustrates the average energy consumption over various pause times of 20, 40, 60, 80, and 100 sec for the TE-AODV, TEAM, and MRAODV protocols at different mobility speeds. The energy consumption is more or less similar for all protocols at a pause time of 20 sec. A faraway node consumes more energy to transmit data than the nearby neighbor node. At a pause time of 60 sec, the TEAM and MRAODV have remaining energies of 93.4% and 94.1%, respectively, whereas the TE-AODV has a higher remaining energy of 95.0%. Figure 3 depicts when the time increases and then the TEAM and MRAODV protocols consume more energy compared with the TE-AODV. Thus, the residual

Table 1. Simulation parameters.

S. No.	Specifications	Value
1.	Number of nodes	100
2.	Area size	1000 m × 1000 m
3.	Packet size	128–1024 bytes
4.	Data rate	2 Mbps
5.	MAC	Wireless LAN (802**.**11)
6.	Traffic source	Constant bit rate
7.	Transmission range	150 m
8.	Queue type	Interface queue **(**IFQ**)**
9.	Antenna type	Omni-directional antenna
10.	Channel capacity	2 Mbps
11.	Simulation time	100 seconds
12.	Pause time	20, 40, 60, 80, 100 seconds
13.	Mobility speed (minimum-maximum)	0–10 m/s

Table 2. Energy model parameters.

S. No.	Specifications	Value
1.	Initial energy	1000 Joule
2.	Transmission power	1.0 watt
3.	Receiving power	1.0 watt
4.	Idle power	0.1 watt
5.	Sleep power	0.05 watt
6.	Transition time	0.001 second

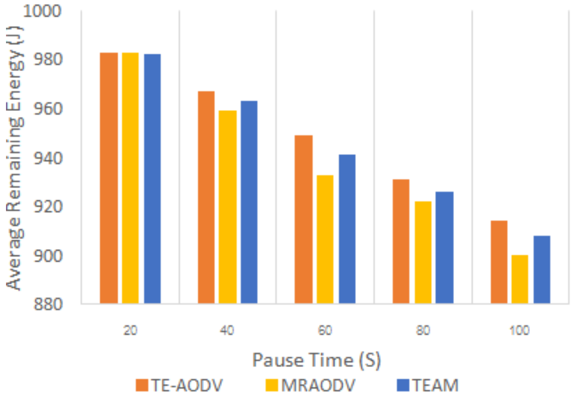

Figure 3. Average remaining energy vs. Pause time.

energy improves up to 5–8% for the mobile node at a pause time of 100 sec. That is the TE-AODV has the higher residual energy of 91.6% compared with the TEAM and MRAODV at 90.1% and 89.4%, respectively. The trust and FPND modules discover the higher energy nodes for routing in the highly dynamic network, whereas the TEAM and MRAODV do not analyze the FPND or trust values. Hence, TE-AODV reserves higher residual energy than other protocols.

Figure 4 shows the performance results of different node densities over PDR. This scenario evaluates the TE-AODV and other protocols over a various number of nodes at different mobility speeds. It shows that as the number of nodes increase, the corresponding PDR decreases slightly for all protocols. The TE-AODV, TEAM, and MRAODV protocols have PDRs of 96.4%, 94.5%, and 93.3%, respectively, at 40 nodes, and the TE-AODV improves the PDR up to 3–5% over the other protocols. As the number of nodes increases to 80, the TE-AODV gives a performance improvement of 5–8% (93% of PDR) compared to the other two protocols, i.e. 89.6% and 90.2%, respectively. The FPND module analysis and involvement of cooperative node demonstrates higher energy and trusted nodes in the route discovery process. Furthermore, it gives a better PDR for the TE-AODV protocol than the TEAM and MRAODV protocols (Figure 4).

Figure 5 illustrates the results of routing overhead for the TE-AODV protocol over TEAM and MRAODV at different numbers of nodes with changing mobility speeds. The TE-AODV protocol significantly improved RO compared with the TEAM and MRAODV protocols at different scenarios. The trust function causes a significant reduction of control packets sent between the source and destination over the network. When the number of nodes is 40, the TE-AODV, TEAM, and MRAODV protocols have ROs of 5%, 8%, 15%, respectively. The trust function improves the RO by delimiting flooding of unwanted control packets in the network, thus it reduces the RO up to 10–12% for the TE-AODV protocol. When the number of nodes increases to 100, the TEAM and MRAODV protocols degrade the network performances by increasing the RO to 38% and 46%, respectively. However, in dynamic networks, the TE-AODV reduces the RO by 7–11%. The improvement differentiates the TE-AODV protocol as better than the other protocols.

Figure 6 presents the RO for the detection of non-cooperative nodes over the number of nodes for the TE-AODV and TEAM protocols. This evaluation considers certain nodes as non-cooperative nodes. The number of non-cooperative nodes is varied from 1–20 randomly in the network. When the number of non-cooperative nodes is 0.2%, then the RO for detection of non-cooperative nodes for both protocols is identical, i.e. 3–4%. Whenever the perception of the non-cooperative node increases, the corresponding RO for both protocols increases (Figure 6). At the perception 0.6%, the TE-AODV has a RO of 15% for non-cooperative node

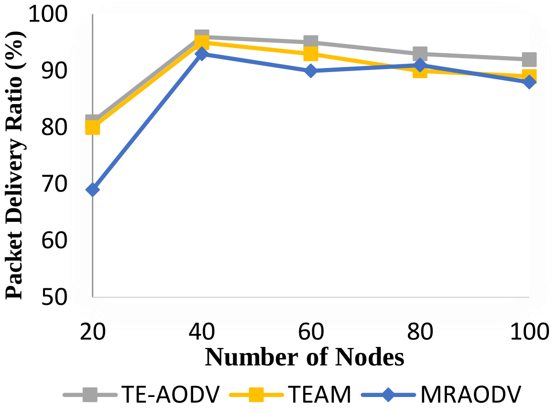

Figure 4. Packet delivery ratio (%) vs. Number of nodes.

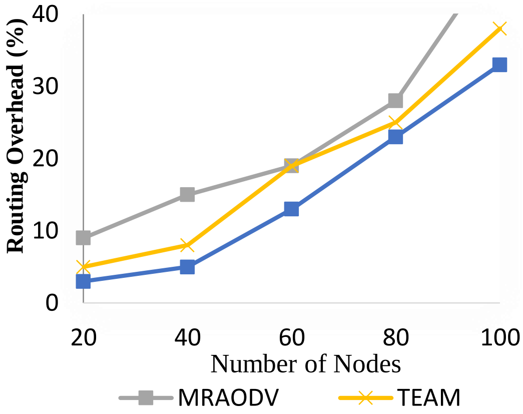

Figure 5. Routing overhead (%) vs. Number of nodes

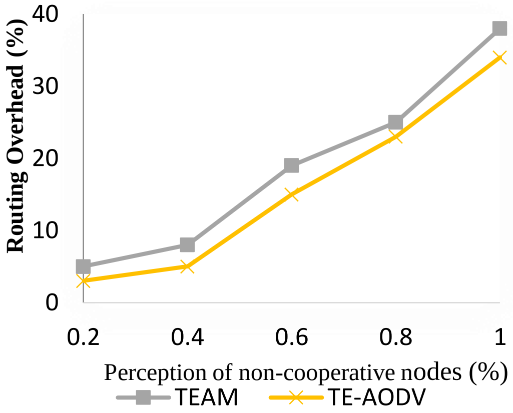

Figure 6. Routing Overhead (%) vs. Perception of non-cooperative node nodes (%).

detection. It is much less compared with the RO of the TEAM protocol, i.e. 21%. At the perception of 1%, the TEAM and TE-AODV protocols have ROs of 39% and 33%, respectively. Since the trust and FPND modules exclude the unwanted flooding of control packets by sophisticated cooperation, the TE-AODV protocol reduces the RO by 6–8% compared with TEAM. The TEAM protocol does not consider the energy and collision parameters.

Figure 7 presents the results of time taken to detect a non-cooperative node over the various perceptions of a non-cooperative node. At a perception of 0.4%, the time taken to detect is similar for both protocols. Afterward, as the perception increases then the corresponding time increases for non-cooperative node detection for both protocols. At a perception of 1%, the TE-AODV protocol has the maximum time gain of 4–8% compared with the TEAM protocol. Since FPND detects in quick time, the TE-AODV protocol takes less time for the detection compared with the TEAM protocol.

Table 3 summarizes the comparative performances of the TE-AODV, TEAM, and MRAODV routing protocols for 60 and 100 nodes. At 60 nodes, the TE-AODV protocol achieves the highest residual energy of 951 J. However, the TEAM and MRAODV protocols have residual energies of 934 J and 941 J, respectively. At 100 nodes, the TE-AODV protocol gives a reduced RO of 33.4%. Nevertheless, the TEAM and MRAODV protocols deliver higher ROs than TE-AODV at 37.9% and 36.4%, respectively.

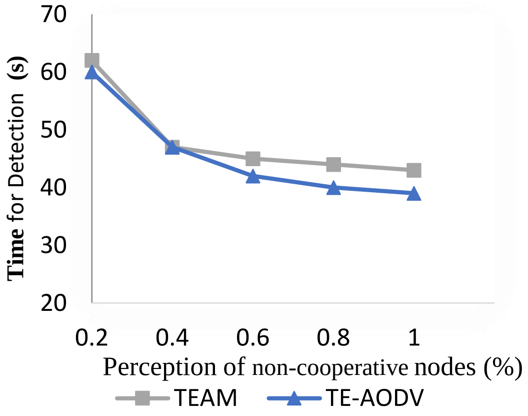

Figure 7. Time for detection (s) vs. Perception of non-cooperative nodes (%).

5. Conclusions

The proposed resource-based TE-AODV protocol provides reliable cooperative communication by using trust and FPND modules for the MANET. The TE-AODV achieves better results for PDR, RO, and remaining energy than the TEAM and MRAODV protocols. The TE-AODV improves the remaining energy of nodes by 5–8%, reduces the RO of nodes up to 8–10%, and gives the maximum time gain of 4–8% in non-cooperative node detection. Henceforth, the proposed TE-AODV protocol offers better resource efficient routing using trust and FPND modules and improves as the number of nodes increases. Moreover, it has reduced energy consumption for routing. Thus, the TE-AODV protocol improves the cooperative communication of the network. For the future, the plan is to enhance the TE-AODV protocol using ANN to predict the futuristic resources of nodes and facilitate routing based on it.

References

Alkhamisi, A. O., & Buhari, S. M. (2016). Trusted secure-adhoc on-demand multipath distance vector routing in MANET. *Proceedings of International Conference on Advanced Information Networking and Applications,* 212-219.

Anderegg, L., & Eidenbenz, S, (2003). Adhoc-VCG: Truthful and cost-efficient routing protocol for MANET with selfish agents. *Proceedings of International conference on mobile computing and networking*, 245–259.

BonnMotion-Tool. A mobility scenario generation and analysis tool. Retrieved from http://sys.cs.uos.de/bonnmotion/

Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2015). Defending against collaborative attacks by Malicious Nodes in MANETs: Cooperative bait detection approach. *IEEE-Systems Journal*, *9*(1), 65-75.

Chong, Z. K., Tan, S. W., & Ng, B. C. K., (2013). Outwitting smart selfish nodes in wireless-mesh-networks. *International Journal of Communication System*, *26*(9), 1163–1175.

Ferraz, L. H. G., Velloso, P. B., & Duarte, O. C. M. B., (2014). An accurate and precise malicious-node exclusion mechanism for ad hoc-networks. *Ad Hoc Networks*, *19*, 142–155.

Fredric, M. H., Imana, E. Y., Allen, W., & Reedy, M. (2009). Reputation prediction in MANET using RBF neural-networks. *Springer*, 485–494.

Gargi, R., Chaba, Y., & Patel, R. B. (2012). Improving performance of DSR protocol by optimization of neural-networks. *International Journal of Computer-Science Issues*, *9*(4), 471–479.

Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehaviour in MANETs. *Proceedings of International Conference on Mobile Computing and Networking*, 255–265.

Table 3. Performance of routing protocols at 60 and 100 nodes.

Protocol	Residual energy (J)		PDR (%)		RO (%)		NC-node detection	
#Nodes	60	100	60	100	60	100	RO (%)	Time (s)
TE-AODV	951	916	95.2	92.3	12.8	33.4	33.5	38.6
TEAM	940	905	92.7	88.6	18.5	37.7	38.8	42.9
MRAODV	933	896	89.9	87.8	19	48.5	-	-

Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black-hole attack in MANET. *Computer and Electrical Engineering, 40*, 530–538.

Ns2Simulator [Computer software]. Retrieved from http://www.isi.edu/nsnam/ns/

Orallo, E. H., Olmos, M. D. S., Cano, J. C., & Manzoni, P. (2015). CoCoWa: Collaborative contact-based watchdog for detecting selfish-nodes. *IEEE-Transactions on Mobile-Computing, 14*(6), 1162-1175.

Pradeep, B. S., & Soumya, M. (2011). Role of ANN in secured wireless multicast routing during dynamic channel allocation for user demanded packet optimality. *International Journal of Advanced Networking and Applications, 11*, 1135–1139.

Prasannavenkatesan, T., & Menakadevi, T. (2016). Significance of scalability for on-demand routing protocols in MANETs. *Proceedings of IEEE Conference on Emerging Devices and Smart Systems*, 76-82.

Prasannavenkatesan, T., Raja, R., & Ganeshkumar, P. (2014). PDA-misbehaving node detection and prevention for MANETs. *Proceedings of International Conference on Communication and Signal Processing*, 1808–1812.

Prasannavenkatesan, T., Rajakumar, P., & Pitchaikkannu, A. (2014). Effective Intrusion Detection System for MANETs. *International Journal of Computer Applications, 3*, 29-34.

Prasannavenkatesan, T., Rajakumar, P., & Pitchaikkannu, A. (2014). Overview of proactive routing protocols in MANET. *Proceedings of International Conference on Communication Systems and Network Technologies,* 173-177. doi:10.1109/CSNT.2014.42

Prasannavenkatesan, T., Udhayakumar, K., & Ramkumar, R. (2014). Security attacks and detection techniques for MANET. *Discovery Journal, 15*(42), 89-93.

Rohini, K. S., & Dhanasekar, S. (2014). Survey on quality analysis of cooperation incentive strategies in MA NET. *International Journal of Computer Science and Mobile Computing, 3*(1), 495-500.

Samian, N., Zukarnain, Z. A., Seah, W. K. G., & Hanapi, Z. M. (2015). Cooperation stimulation mechanisms for wireless-multihop-networks. *Journal of Network and Computer Applications, 54*, 88–106.

Shakshuki, E. M., Kang, N., & Sheltami, T. R. (2013). EAACK: Secure-IDS for MANETs. *IEEE Transactions on Industrial Electronics, 60*(3), 1089-1098.

Zarei, M., & Faez, K. (2012). Modified Reverse AODV Routing Algorithm using Route Stability in MANET. *Proceedings of International Multitopic Conference*, 255–259.