International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

# EDTDS-AODV: An Enhanced Distributed Secure Routing using Trust Model with Improved D-S Evidence Theory in Manets

**M. Vijaya Bhaskar, N. Geethanjali**

***Abstract--- Mobile Ad Hoc Networks (MANETs) is a group of mobile nodes with a dynamic (changing) topology and it works under scalable conditions for many applications and cause various security dispute. Recognizing the misbehavior is a tedious issue, because of the nomadic nature of nodes. For recognizing the destination route, nodes will share the routing details between the neighbors. So, nodes should trust one another, and here, trust is the main thing in secure routing mechanism. The MANETs current routing protocol concentrates on recognizing the paths in the dynamic networks without considering security. Here, an enhanced distributed trust model which computes neighbours' direct trust by factors of encounter time, mobility, energy, successful cooperation frequency and some other more. In order to link the multiple recommended pieces of evidence and obtain the recommended trust value, we make use of the enhanced Dempster-Shafer evidence theory. EDTDS-AODV protocol is proposed in our work by extending the AODV protocol, which works according to the novel trust mechanism, an enhanced distributed trusted secure routing protocol. Here, based on the trust values of its neighbour nodes, the node decides the routing decision. And at last, proposed method modifies the traditional AODV routing protocol with the constraints of trust rate, energy, and mobility etc., according to the malicious behavior prediction. The trust rate is defined by the packet sequence ID matching from the log reports of neighbor nodes, which eliminates the malicious report generation. The trust level is increased by using the direct and indirect trust observation schemes. The trusted node is checked whether it is within the communication range or not, with the help of received signal strength indicator. From the experimental result it is confirmed that the EDTDS-AODV can avoid the malicious nodes effectively when building the route; in addition, it also accomplishes the better performance when compared with TAODV and AODV with respect to throughput, packet delivery ratio, and average end to end delay.***

***Keywords: Mobile ad-hoc network (MANET), Ad Hoc On-Demand Distance Vector (AODV), Distributed Trust management, Improved D-S evidence theory, Expected Transmission Count (ETX), Path encounter Rate (PER), Average Encounter Rate (AER), Successful Cooperation Frequency (SCF)***

## I. INTRODUCTION

Trading the subtleties without brought together position and fixed foundation is finished by a versatile specially appointed system (MANET) is a self-governing arrangement of remote portable hubs that powerfully structure a system. On account of restricted correspondence range and asset limitations of the hubs, portable hubs cooperate with each other in a multi-jump way for accomplishing the information transmission. Each hub functions as host, without switch and furthermore as a remote switch to advance bundles for different hubs that might be outside its correspondence extend [1].

On the off chance that on the off chance that whole hub works in a benevolent manner, at that point the system capacities well. MANETs are especially defenseless against various kinds of directing assaults propelled by inward hubs [2], as a result of the transparency in system topology, disseminated nature and absence of focal power. Thus, this outcomes in different difficulties in steering, when recognized with the customary remote systems. The conventional directing conventions proposed for impromptu systems are adequate in managing different steering assaults. As the headways in inescapable remote systems are at point of confinement, MANETs has pulled in the consideration of the scientists around the world as of late. Normally hubs don't rely upon a focal hub to arrange with one another, in MANET; rather they work in a co-usable way so as to convey the information between hubs [3], which are a long way from each other's. In this way, whole hubs in the system ought to keep up and distinguish their individual courses to the goal hubs. Her, hubs have obliged assets like constrained battery, data transfer capacity and a high versatility factor [4], which recognize MANETs from different remote systems [5]. Despite the fact that it has these issues, MANETs are generally utilized at times where the speed of system usage is profoundly required with no pre-built structure ahead of time, for example, military correspondence, crisis correspondence and portable conferencing [6, 7]. Barely any well known steering conventions like Ad-hoc on-request separation vector (AODV) [8], dynamic source directing (DSR) [9], and so forth, were used to set up the system of portable hubs, for finding the trusted and ideal way between hubs. The thought of trust would affirm to be valuable for dynamic situations where the hubs required relying upon one another to achieve their objectives [10]. Secure convention utilizing trust system called effective secure directing convention, was recommended by Bose et al. [11]. Trust has been built up with the assistance of marked affirmation dependent on unbalanced key cryptography. Be that as it may, it won't cover the Key dissemination issue.

Manuscript published on 30 September 2019
* Correspondence Author
**M. Vijaya Bhaskar***, Research Scholar, Department of Computer Science and Engineering,Rayalaseema University, Kurnool
**N. Geethanjali,** Professor, Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapur

The trust model to verify the AODV directing convention, was proposed by Sharma et al. [12]. Trust mix calculations and trust mapping capacities are the arrangement of trust count. By including the trust data the steering table and the directing messages can be adjusted.

A trusted steering plan with example revelation (TRS-PD) was formulated by prior work [13],that consolidates the trust model (in light of QoS trust parts) with an assault design disclosure instrument for perceiving the malignant hubs sooner than a lone trust model. A trust based steering convention named Enhanced Average Encounter Rate-AODV (EAER-AODV) is proposed in [14], which authorizes the trust model dependent on hubs' assessment. Be that as it may, this work further expands the assessment of vitality utilization of every hub and its exchange off with the security components. This key thought rouses the scientists to recommend the novel trust system called an upgraded circulated believed secure steering convention with an improved D-S proof hypothesis is proposed EDTDS-AODV convention by expanding the AODV convention. In view of the trust estimations of its neighbor hubs, the hub settles on the directing choice. The principle specialized commitments of this work are as per the following:

- An upgraded trust model is proposed for AODV convention has two components which make the trust system

progressively fitting for asset limited MANET. First is the improved D-S proof hypothesis, which processes the immediate trust esteem, incorporates circuitous proof, and gain the general trust esteem.

- Second is a hub assesses its neighbors' trust worth dependent on the trust model and it pick the solid hubs as its next-jump hubs.
- The proposed EDTDS-AODV directing model empowers hubs to adjust steering measurements (i.e., Energy, ETX, PER, AER and SCP), to the system portability states (i.e., static, versatile individually) in view of the identification above.

- Simulations continue to recognize the presentation of EDTDS-AODV affirms that the exhibition of MANETs upholding the EDTDS-AODV is more prominent when contrasted and the MANETs utilizing TAODV and AODV against particular kinds of enemies.

The rest of the piece of the section is sorted out as pursues. The related work of trust based security model in MANET is talked about in area 2. In Section 3, the proposed trust model is talked about with the upgraded trust-dependent on interest directing plan consolidated into AODV convention is examined in Section 4. Area 5 presents activities performed by different foe models and the recreation results delineating the exhibition of ETRS-PD is displayed. Finally, Section 6 closes the part.

## II. RELATED WORK

In Ad hoc organizes, using the trust and choosing a believed course for parcel transmission is a huge element. Perceiving the vindictive hubs in the way of steering and to evade the foes from publicizing themselves as great is the objective of trust foundation instrument. For secure steering, different specialists proposed distinctive trust assessment models. Here, we clarify the distinctive Routing convention in MANET and recognize among three conventions as Reactive, Proactive and Hybrid, premise of different parameter as directing way of thinking, steering plans, directing overhead, dormancy, and adaptability level. This present area's yield is hypothetical and it picks the convention as per prerequisites. The rest of the piece of this segment focuses on security of MANET convention under different steering assault since security is the primary test on MANET [15]. The detail investigation of various steering assaults in MANET is portrayed in [16]. The security is most questions in Mobile impromptu arrange (MANET) under different steering assault, on account of open nature of versatility. Future Work focuses on Security in MANET and gives a security under different assaults.

The security is packed in [17], with the assistance of various cryptography strategy for security and recognize among the symmetric calculations, for example, AES and Blowfish and Asymmetric calculations like RSA and ECC utilized for verification. The yield says that: ECC (Elliptic bend Cryptography) is superior to RSA. The other security methods in Cryptographyis clarified further. The different directing conventions in MANET and different Routing assaults in MANET with different security plans, was depicted by Suman Bala, Er.Amandeep Singh Bhandari and Dr. Charanjit Singh (2017). Distinctive sort of steering assault present in the MANET as the working of different security conventions is clarified in this work. We can perceive the better arrangement of these sorts of different assaults, utilizing security conventions. These security conventions were executed in MANET to limit the impact of the assaults [18].

The trust based security directing with trust in different points of view in MANET was inspected in [19]. It is monotonous to deal with the trust based security in MANET, due to its open nature; it is the essential debate of MANET. Whole plausible trust the board for secure directing with essential conventions was analyzed here. So as to approve the estimations of a trust, it registers the trust and social networks. Effective Trust based steering utilizing difficulties to build up security was recommended in [20]. This takes the plan from this present reality system of companions. IT will isolate the vindictive hubs which are left with no pretend. The principle disadvantage here is: it doesn't depend on any plan that will spread data about the malevolent hub so the odds of impacting happens are exceptionally low. The exceptional test is in confirming the hubs one of a kind attributes.

Secure Zone directing Protocol (ZRP) was proposed in [21], for perceiving the making trouble hubs and keep arrange from wrecking. Neighbor Discovery Protocol (NDP) recognizes the neighboring hubs in the remote station thinking about its area and round excursion data, in MANET. Parcel uprightness is given in Secure Intra Zone Routing Protocol (SIERP), which uses the RSA and advanced mark.

Trust Based Secure On Demand Routing Protocol (TSDRP) was recommended in [23], where the Adhoc on interest Distance vector (AODV) is changed to propose TSDRP to verify it from different assaults like Black gap assault, Denial of administration assault and so forth. Be that as it may, this convention gives insurance from these assaults. AODV was altered to TSDRP by presenting Node Trust Table (NTT) and Packet Buffer (PB).

In [23], we use the component to perceive the impacting hubs through observing of the conduct of hubs and recognize the conduct with got notoriety esteem in an alarm message. As Collude hubs are recognized they are disposed of for further correspondence. So as to satisfy the security requests, prior, DTMAC was proposed, yet tragically it faces various dangers from malignant hubs. One and more individuals from the impacting bunch part need to aggravate the system for securing the trust based condition against crash assault, which perceives the colluders and rebuff them. We can perceive the colluders and rebuff them by disposing of the impacting CH and keep them from further interest in the system correspondence by checking the conduct of hubs.

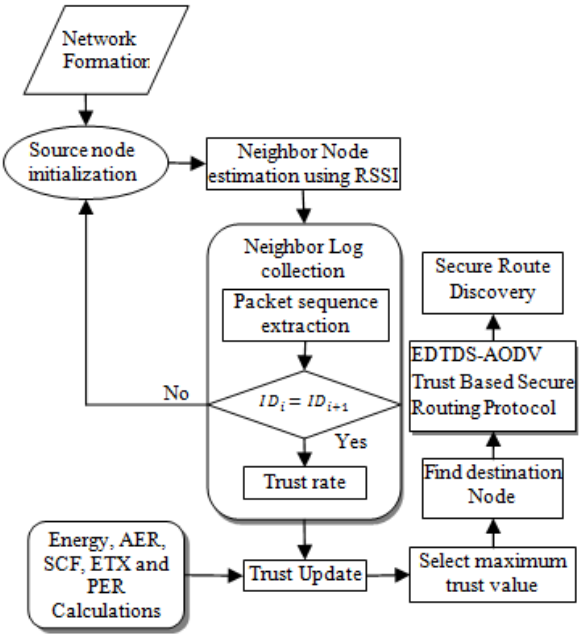
A companionship based trust based model for secure directing from source to goal was proposed in [24], so as to demonstrate the level of hub dependability we bring the various degrees of kinship. This redresses the downsides of disregarding the social conduct of the vindictive hub. We utilize foresee hubs conduct for future correspondence, so as to make an interpretation of the proof in to assessment. A scientific model is included for this trust supervisor. An approach chief empowers distinctive choice principles and arrangements.

Evaluation Trust secure directing dependent on trust levels was recommended in [25], which upgrades the parcel conveyance proportion with the assistance of trust to disconnect Black opening assault and offer secure steering for information traffic. In the system, we register the proportion if powerful parcel exchange among the neighbor hubs. Evaluation trust convention will be ordered based on the significance of the trust level of the hub, as indicated by the proportion hubs in the system. It proceeded till the parcel achieves the goal.

Dissimilarity directing with keeping up and overseeing of a current secluded security Architecture is affected and coordinated, and this thought is clarified in [26]. BY receiving the Adhoc On-level Demand Multipath (AOMDV) Trust and unwavering quality, we can accomplish the dispersity steering, since the parameters used with numerous courses gives a reviewed directing administration − the capacity of giving a few potential courses to a goal in a MANET, every one of which might be chosen since its security and dependability measurements coordinate those of the approach.A trust mechanism is suggested in [27], for protecting the AODV protocol. The ant agent put positive pheromone, when the node is trusted. Path communication works according to this pheromone. The performance improves with respect to packet delivery ratio and throughput. An algorithm for trust evaluation of every node and trust computation metric based on node's impulsive behavior to became, malicious in dynamic environment was suggested in [28]. A trust model is defined which helps in node authentication and it evaluation function helps to measure the trust value based on experiences. A trust relationship function was defined, to combine blind trust value and referential trust value. In this section many schemes are analyzed and surveyed in MANET for giving the trust based secure routing to ensure the trust in multiple perspectives. Open nature makes it tedious to maintain the trust and resource constraints; hence the trust is the preferred challenge for best performance. Here we examine the entire feasible trust management for secure routing with necessary protocols. The trust to be computed and social communities helps to check the computation of trust and it is appropriate in dynamic topology, which is allocated to the network like MILITARY but with certain constraints such as maintaining reliability, scalability, re-configurability.

## III. PROPOSED TRUST MODEL BASED ROTING

Successful participation recurrence is proposed in this trust system, which is expected in the immediate trust assessment to ensure arrange security. The system topology in MANET is dynamic, along these lines, it produces the vindictive free stable system, here; we acquired the normal experience rate as one of the measurement in direct trust assessment further to fruitful participation recurrence. So as to figure the immediate trust an incentive by consolidating aberrant proof and thus get generally speaking trust esteem, Improved D-S proof hypothesis was used here. By broadening the AODV convention named as EDTDS-AODV, we further set forward the trust based directing convention. A hub registers its neighbors trust worth dependent on the trust model and chooses solid hubs as its next-bounce hubs, in this convention. The hub whose trust worth is over the trust edge is considered at last to end way among source and goal hub. Additionally, the proposed strategy changes the conventional AODV steering convention with the requirements of Energy, normal experience rate (AER) and fruitful participation recurrence (SCF), Expected Transmission Count (ETX), Path experience Rate (PER) based vindictive conduct forecast. The trust rate that stays away from the vindictive report age was characterized by the parcel succession ID coordinating from the log reports of neighbor hubs. . Also, the immediate and circuitous trust perception plans helps in expanding the trust level. The got sign quality marker helps in characterizing the believed hub is inside the correspondence extend or not. In fig.1. Trust model basically performs trust determination, calculation, and application and the general procedure is given. Further we examine the Trust applications including trust based course disclosure and course determination.




**Neighbor log collection**

With the assistance of RSSI based separation estimation, a source hub is chosen and the neighbor hub is removed. Further, the trust estimation of the hub is refreshed by the vitality model computation, bundle arrangement ID coordinating rate and versatility estimation. A hub having greatest trust worth was picked as a middle hub for parcel move to the goal hub. Regarding PDR, throughput, normal deferral, the quantity of false positives, we register the proposed plan. To the neighbor log gathering calculation, the hubs and the chart were given as info esteems. For the info hub, the neighbor hub rundown is assembled at first. Further, the subtleties were assembled from the log reports of the considerable number of hubs took part in the protected information move. The parcel arrangement ID of the specific hub is extricated from the log reports. At that point, RSSI techniques evaluates the separation [29], if, on the off chance that the processed separation worth is less when contrasted and the correspondence run, at that point we recognize the parcel ID of the present hub with the ID of next hub. On the off chance that, in the event that, both are equivalent, at that point the particular trust rate is evaluated as given in segment 3.1. At that point table 1 shows the meaning of factors utilized in neighbor estimation calculation. So as to gauge the trust estimation of the hub, neighborhood estimation is the fundamental advance. The hubs closer to the source hub were perceived by RSSI-based separation. The area hubs are determined utilizing the accompanying calculation:

**Table 1: Neighbor Estimation Algorithm Using RSSI**

Input: Node (N), Graph
Output: Trust Rate $TR_i$
Step 1: Collect the Neighbor Node (NN) list of input node (N)
Step 2: Collect the log information of specific NN (Log_N(i) )
Step 3: Get the packet sequence IDs from the log reports of nodes
Step 4: For i = 0 … n then//where n = Network Size
Step 5: Calculate $d_{s,i}$ using $d_{s,i} = RSSI(N, G_i)$
Step 6: if($d_{s,i}$< Range) then
Step7:
$PACKET\_ID_{N(i)} =$
$Extract\ ID\ of\ packets\ (Log\_(N(i)+1))$
$PACKET\_ID_{N(i)} == PACKET\_ID_{N(i+1)}$
Step 9: Compute trust rate as $T_i$
Step 10: Else
Step 11: Goto step 1
Step 12: End if
Step 13: Else
Step 14: Goto step 1
Step 15: End if
Step 16: End ForStep 8: If

operations seamlessly. Encounter rate indicates the set of new encounters (nodes) that a mobile node A experienced during time duration T from $T_i$ (indicated as incident time of encounter) to $T_{i+1}$[30]. Average encounter rate (AER) of node is determined as the average number of new encounters per time unit T, which is calculated as follows:

$$AER_S = \frac{|E_S|}{T}$$

In above equation, where $|E_S|$ is the cardinality of the set $E_S$ or the number of elements of the set $E_S$. Theoretically, higher value of $AER_S$ indicates less trusted nodes compared to the nodes having lower value.

## IV. SUCCESSFUL COOPERATION FREQUENCY (SCF):

$$SCF_{i,j} = \frac{f_{i,j}}{f_{i,j} + d_{i,j} + w_{i,j}}$$

Hence, the routing path is chosen as follows:

$$P_{selected} = \underset{P_j}{\operatorname{argmin}}(SCF_{i,j})$$

where □□ is the set of available paths connecting the source and the destination.

**Expected Transmission Count (ETX):** Here, the ETX metric is modified with the network mobility state where the criteria to cost a path changes respectively. That is, in static condition, nodes employ ETX metric for routing, which is computed at each node as follows:

$$ETX = \frac{1}{Df_{i,j} \times Dr_{i,j}}$$

Where $Df_{i,j}$ is indicated as the forward delivery ratio which indicates the probability of successful packets which is received; $Dr_{i,j}$ is the reverse delivery ratio which indicates the probability of successful acknowledgement packets which is received; $ETX \geq 1$, the source node should choose the lowest ETX path (denoted $P_{selected}$) for routing between entire available paths $P_j$ from the source to the destination.

$$P_{selected} = \underset{P_j}{\operatorname{argmin}} \left( \sum_{i=1}^{m} ETX \right)$$

where $m$ is the number of links along the routing path; $P_j$ is the set of available paths connecting the source and the destination. This process gives a highest through path for nodes to route packets across the network [32].

**Path Encounter Rate (PER): F**or routing [30], our earlier works gives mobile condition, nodes employ Path Encounter Rate (PER), a new path routing metric. The PER of a path is determined as a sum of squared Average Encounter Rates (AER) of all nodes along to the path calculated as follows:

$$PER = \sum_{i=1}^{m} AER_{S_i}^2$$

where $m$ is the number of nodes along the routing path. Since AER reflects the relative mobility of a node when distinguished with others around, the path which has the lowest PER is the most stable path. By doing so, packet will be routed over the most stable path in a high dynamic network caused by node movement, in order to minimize the link breakage rate hence minimizing the number of lost packets. Hence, the routing path is selected as follows:

$$P_{selected} = \underset{P_j}{\operatorname{argmin}}(PER)$$

where $P_j$ is the set of available paths connecting the source and the destination.

**Direct Trust:** Query node $i$ observes the behaviors of target node $j$ and computes the corresponding direct trust $DT_{i,j}$ with the help of the formula provided as follows: $DT_{i,j} = (\omega 1 \times E_{i,SN}) + (\omega 2 \times AER_S) + (\omega 3 \times SCF_i, j + (\omega 4 \times ETX) + (\omega 5 \times PER)$
where ω1-ω5 ,are predefined weights in the range [0,1] for cooperative and non-cooperative behaviors.

### 1.1. Improved D-S evidence theory for Recommended Trust

The DempsterShafer theory [33] is a mathematical theory which links evidence from various sources and arrive at a degree of belief which is indicated by a belief function that considers all the available evidence, which is nothing but the generalization of the Bayesian theory of subjective probability, here we have various situations enforcing the ambiguity in which the theory of probability isn't helpful. Dempster Shafer theory is an approach to manage the uncertain knowledge. Entire feasible mutually exclusive events of the same kind are enumerated in the frame of discernment Θ. For example: every node $i$ contribute its opinion about target node j by allocating the belief over Θ.The assignment function is called as the Basic Probability Function (BPA) or the Mass Function $m$: $2^{\Theta} \rightarrow [0,1]$ of the node $i$, denoted by $m_i$. Based on the node $i$ observation, the probability that the target node $j$ is trusted is represented by a confidence interval $[Belief_i(T), Plausibility_i(T)]$.

$$\Sigma m(A) | A \subseteq \Theta = 1, m(\emptyset) = 0$$

The belief function that supports the target node j is 'Trusted is defined as:

$$Belief_j(T) = \Sigma_{A \subseteq T}\, m(A)$$

Plausibility confidence which accounts entire observations that adds the given proposition:

$$Plausibility_j(T) = 1 - \Sigma_{A \subseteq T = \emptyset}\, m(A)$$

For every possible proposition say 'Trusted the D-S rule of combination is enforced to combine node $i$ observations $m_i$ and node $j$ observation $m_j$.

$$m_1 \oplus, \ldots, \oplus m_5(T) = \frac{\sum_{A \cap A_{k'=A}} m_i(A_k) \cdot m_j(k')}{\sum_{A \cap k'=A} m_i(A_k) \cdot m_j(k')} \forall i = 1, j = 2 \; to \; 4$$

However in our trust model, weights are allocated for computing the recommended trust based on the five factors about the target node □ and thus acquired the following:

$$RT_{i,j} = m_1 \oplus, \ldots \oplus, m_5(T) = \frac{\sum_{A \cap A_{k'=A}} [\omega_i m_i(A_k) \cdot \omega_j m_j(k')]}{\sum_{A \cap A_{k'=A}} \omega_i m_i(A_k) \cdot \omega_j m_j(k')} \forall i = 1, j = 2 \; to \; 4$$

Total Trust Evaluation: The overall trust is evaluated by combining direct observation of node $i$ about node $j$, that is, $DT_{i,j}$ and recommended observation of the neighboring node m about target node $j$.

$$TT_{i,j} = DT_{i,j} + RT_{i,j}$$

### 1.2. Trust Based Secure Routing Protocol: EDTDS-AODV

By recognizing the trusted end-to-end path free of malicious nodes, we got the motivation to design the trust based secure routing. We extend the AODV protocol here, though which we can develop the trusted route with maximum path trust based on trust mechanism indicated by EDTDS-AODV. The basic concept here is: checking the trust level of the node by transmitting the route request packet. Paths with maximum trust levels were chosen by the source node to transmit the packet to the destination node as the end-to-end path. According to the EDTDS-AODV protocol, secured route is developed by the trusted path. Table 2 indicates the proposed EDTDS-AODV protocol.

**Table 2: Trust Evaluation Algorithm EDTDS-AODV protocol**

| |
|---|
| Input: Node (N), Graph |
| Output: Routing with trust value |
| 1 node $i$ computes trust value of node j $DT_{(i,j)}$ |
| 2 if $DT_{(i,j)} > T_{tr}$ (trust threshold) then |
| 3 node $i$ computes total trust $TT_{i,j}$ of node $j$, using direct trust $DT_{i,j}$ and recommended trust $RT_{i,j}$ |
| end |
| 4 else |
| 5 node $i$ regard node $j$ as 'Distrust' end |
| 6 if total trust $TT_{i,j} > T_{tr}$ then |
| 7 node $i$ regard node $j$ as 'Trusted' end |
| 8 else |
| 9 node $i$ regard node $j$ as 'Distrust' |
| end |

**Route Discovery:** Suppose node $i$ has to broadcast the packet to node $d$. Node $i$ begins the route establishment process by transmitting route request packet to its neighbors.

At the time of process of route discovery, when node $i$ selects the node j to forward the packet, node i might suffer from malicious behavior of node j like black hole attack. Hence, it is required to choose a reliable next hop node.

The process of judging whether node j can be the next hop of node $i$ is as follows.

Step 1: Node $i$ verifies whether it has the trust value of node $j$ if $TT_{i,j}$ ; if it has, go to step 7, else, go to step 2.

Step 2: Node $i$ evaluates $DT_{(i,j)}$ and broadcast a Recommendation Query message to the common neighbors denoted as m.

Step 3: After receiving the Recommendation Query message, node m transmits $DT_{(m,j)}$ to node $i$.

Step 4: After receiving the recommended piece of evidence from the neighboring nodes m, node $i$ computes $RT_{i,j}$ and $TT_{i,j}$

Step 5: if $TT_{i,j} > T_{tr}$ (trust threshold), node j transmit a route reply packet to node $i$ through backward path.

Step 6: Node j rebroadcast route request packet to its neighbor having $TT_{i,j} > T_{tr}$ and also it sets up a reverse route to the sender.

Step 7: check whether node $j$ is reliable and it can be estimated with the help of Algorithm 1. If node $j$ is trusted, node i will select the node j as the next hop node, else node $i$ won't select the node j to broadcast the packets and put node j into its local black list as a malicious node.
Once a node is in a black list, it can neither receive any packets from its neighbors not it can forward any packets. Which mean:, when a node is in the black list, it is not added in the local network. In the proposed scheme, the trust threshold $T_{tr}$ is considered as 70%. In this way route request packet reaches from source to destination by avoiding untrustworthy node.

## V. RESULTS AND DISCUSSION

We expect 70 portable hubs in our reproduction which are arbitrarily set in a 1000 × 1000 square field. Whole hubs explore freely following arbitrary waypoint model and the speed varies from 5 to 30 m/s. The transmission scope of each hub is set to 250 m. In reproductions, the quantity of vindictive hubs contrasts from 5 to 30. At the point when a parcel is gotten by a malignant hub, it either drops or specifically advances the bundle to a hub. Subsequently, malignant hub carries on like a blackhole hub. Such pernicious conduct is incorporated to the AODV convention, for looking at the exhibition of our strategy. Arbitrary hubs were picked to play out the malignant movement by dropping bundles. In this segment considered four measurements for estimating the presentation of the proposed EDTDS-AODV: (I) Throughput: number of parcels gotten by the goal hub per unit time. (ii) Packet Delivery Ratio (PDR): the proportion of the quantity of bundles got to the all out number of parcels. (iii)Detection Accuracy: the quantity of malevolent SNs recognized from the absolute number of vindictive SNs present in the system. (iv) Energy utilization: the absolute vitality devoured for finishing the fruitful information transmission and (v) Routing Overhead: number of steering bundles got partitioned by the all out number of information parcels. The proposed strategy EDTDS-AODV is recognized with the condition of-specialty of TAODV and AODV strategies for processing the exhibition of the proposed methodologies, a few parameters were used like Throughput, Packet Delivery Ratio (PDR), Detection Accuracy (DA), Energy Consumption, and Routing overhead. This work expect the accompanying huge Performance measurements for the assessment by reenactment. Here proposed EDTDS-AODV model is contrasted and the ebb and flow investigate strategies TAODV and AODV.

### 4.1. THROUGHPUT (TP)

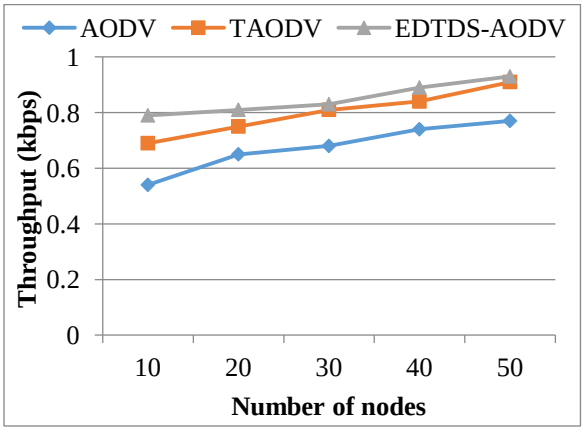



**Fig.2.Throughput vs. No of Nodes**

Fig.2 gives the comparison result of throughput from the proposed EDTDS-AODV, and the current TAODV and AODV method. It is stated that the proposed EDTDS-AODV acquires the greater throughput when distingusihed with all the other proposed and current approaches like TAODV and AODV. The performance of throughput by nodes is observed to be still greater for further increasing nodes too. The reason is that, the proposed work has the ability to recognize the malicious nodes in a good trust management system which leads the throughput would be greater with neighbor log collection database.

### 4.2. Packet Delivery Ratio (PDR)

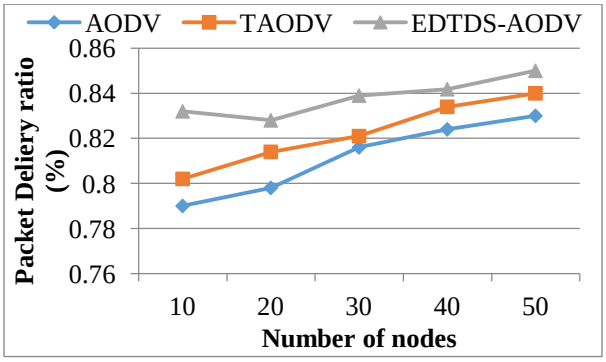



**Fig.3.Packet Delivery Ratio vs. No. of Nodes**

The delivery ratio is given in the Fig.3 it is simply the ratio of the number of delivered and broadcasted message to the destination node. It is usually provides the report of transmitted message to the destination node. It can be stated: that the proposed EDTDS-AODV approaches have a greater ration of transmitting the packets when distinguished with the TAODV and AODV approach. From the figure it is provided that,

when number of nodes maximized the suitable delivery ration also maximizes steadily. The proposed EDTDS-AODV is having high delivery ratio when distinguished with the current methods. The reason is that, the proposed work can recognize the trustworthy nodes in its neighbor with the help of improved DS theory.

### 4.2. Detection Accuracy

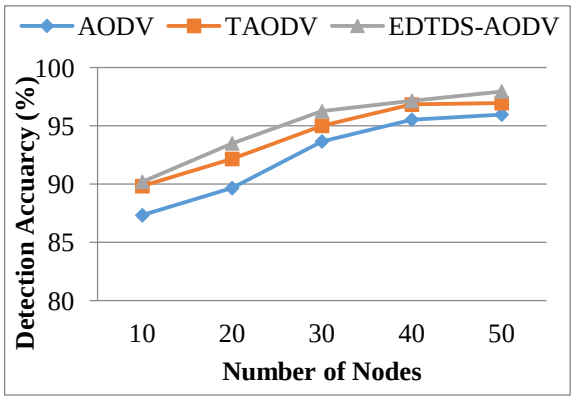



**Fig.4.Detection Accuracy Vs No. of Nodes**

Fig.4 provides the combined malicious node detection accuracy of TAODV, AODV and EDTDS-AODV scheme under various kinds of attacks. It is observed that the detection accuracy of EDTDS-AODV is higher when compared with TAODV and AODV scheme under different attacks. From fig.2, it is observed that when the number of malicious nodes maximizes in the network, the average DA gets minimized. When trust management system is executed, the average detection accuracy of EDTDS-AODV, TAODV and AODV, are 97.95%, 96.95% and 95.97% correspondingly. Te reason is that; it enhances the reliability of route discovery when distinguished with the traditional trust mechanism.

### 4.3. ENERGY CONSUMPTION

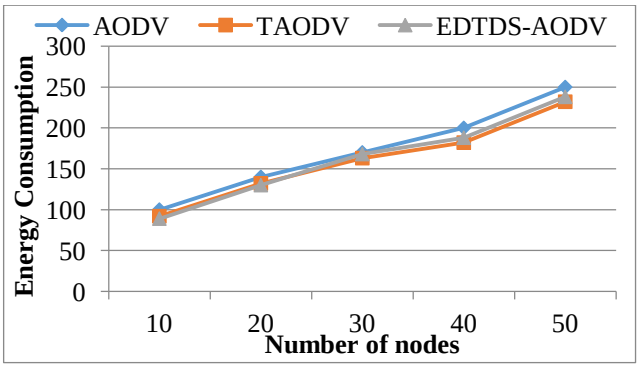



**Fig.5. Energy consumption Vs No. of Nodes**

Fig.5 shows the relationship among the Energy consumption on communications and the number of nodes. It can be stated that the proposed EDTDS-AODV approach takes less energy when distinguished with the other TAODV and AODV approach. From the figure, the energy value will minimize predominately when malicious nodes initiate attacks in WSN. EDTDS-AODV can maximize the energy value when distinguished with TAODV and AODV, since it assumes the direct trust, indirect trust and incentive factor, which can oppose error detection efficiently.

### 4.4. Routing Overhead

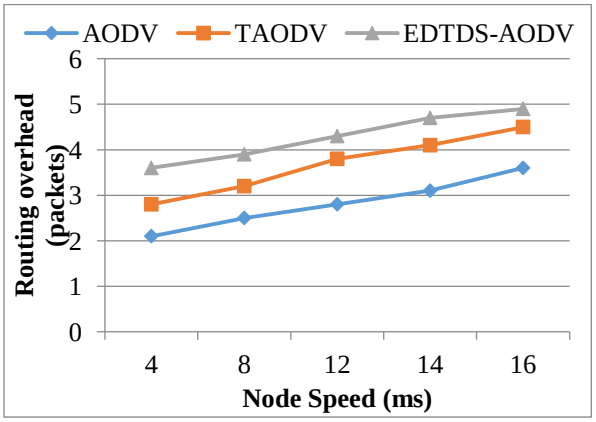



**Fig.6. Routing Overhead vs. No of Nodes**

Figure 6 provides the average routing hop of EDTDS-AODV, TAODV and AODV with various numbers of malicious nodes. when the number of malicious nodes accounts for a specific proportion of the number of total nodes, the average route hop of EDTDS-AODV is a greater when compared with that of TAODV and AODV, since nodes would rather select the relative longer path instead of selecting the malicious nodes as the next hop nodes in other current methods. Though the path of EDTDS-AODV may be a little longer, the performance of EDTDS-AODV is still better when compared with that of TAODV andAODV as it avoids the malicious nodes out of the routing paths.

## VI. CONCLUSION

An epic trust based AODV steering system named EDTDS-AODV is recommended in this work for MANET. Here, the possibility of vitality, AER, SCF, ETX and PER is considered in trust assessment, which is resolved dependent on the hubs conduct. Meanwhile, the improved D-S proof hypothesis consolidates prescribed data to obtain the general trust esteem. Through the broadening the AODV convention, a trusted steering convention dependent on the novel trust metric is displayed. Finally, the proposed EDTDS-AODV is recognized with AODV and TAODV by looking at the presentation measurements. Reenactment result expresses that the proposed EDTDS-AODV is recognized with AODV and TAODV by looking at the exhibition measurements. Besides, the proposed work achieves the upgrades in the parcel conveyance proportion and despite the fact that throughput is undermined however the plan could ready to isolate the noxious hub and boost the lifetime of the hubs in the system. In future, thorough execution assessment will be done when contrasted and the EDTDS-AODV with other steering convention, for example, DSR and OLSR.

## REFERENCES

1. Junhai, L., Danxia, Y., Liu, X. and Mingyu, F. A survey of multicast routing protocols for mobile ad-hoc networks. IEEE Communications Surveys & Tutorials. 2009;11(1):78-91.
2. Xia, H., Jia, Z., Ju, L., Li, X. and Sha, E.H.M. Impact of trust model on on-demand multi-path routing in mobile ad hoc networks. Computer Communications. 2013;36(9):1078-1093.

3. Njilla, Laurent, Harold Ouete, Niki Pissinou, and Kia Makki. "Game theoretic analysis for resource allocation in dynamic multi-hop networks with arbitration." In Systems Conference (SysCon), 2017 Annual IEEE International, pp. 1-8. IEEE, 2017.
4. Pathan, Muhammad Salman, Nafei Zhu, Jingsha He, Zulfiqar Ali Zardari, Muhammad Qasim Memon, and Muhammad Iftikhar Hussain. "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs." Future Internet 10, no. 2 (2018): 16.
5. Mandhare, V. V., V. R. Thool, and R. R. Manthalkar. "A novel approach to improve quality of service in MANET using cache update scheme for on-demand protocol." International Journal of Communication Networks and Distributed Systems 18, no. 3-4 (2017): 353-370.
6. Anjum, Shaik Shabana, Rafidah Md Noor, and Mohammad Hossein Anisi. "Review on MANET based communication for search and rescue operations." Wireless Personal Communications 94, no. 1 (2017): 31-52.
7. Sandeep, J., and J. Satheesh Kumar. "Efficient packet transmission and energy optimization in military operation scenarios of MANET." Procedia Computer Science 47 (2015): 400-407.
8. Anand, M., and T. Sasikala. "Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol." Cluster Computing (2018): 1-7.
9. Prabha, Jyoti, Dinesh Goyal, Savita Shivani, and Amit Sanghi. "Prevention of Conjunct Black Hole MANET on DSR Protocol by Cryptographic Method." In Smart Trends in Systems, Security and Sustainability, pp. 233-240. Springer, Singapore, 2018.
10. Yu, H., Shen, Z., Miao, C., Leung, C. and Niyato, D. A survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE. 2010;98(10):1755-1772.
11. Bose D, Banerjee A, Bhattacharyya A, Saha H, Bhattacharyya D, Banerjee P. An efficient approach to secure routing in MANET. In Advances in Computing and Information Technology, Advances in Intelligent Systems and Computing, Meghanathan N, Nagamalai D, Chaki N (eds.). Springer: Berlin Heidelberg, vol. 176, 2012; 765–776, DOI:10.1007/978-3-642-31513-8_78.
12. Pankaj S, Yogendra KJ. Trust based secure AODV in MANET. Journal of Global Research in Computer Science 2012; 13(6).
13. Jhaveri, R.H. and Patel, N.M. Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. International Journal of Communication Systems. 2016; DOI: 10.1002/dac.3148.
14. Mukherjee, Saswati, Matangini Chattopadhyay, Samiran Chattopadhyay, and Pragma Kar. "EAER-AODV: Enhanced Trust Model Based on Average Encounter Rate for Secure Routing in MANET." In Advanced Computing and Systems for Security, pp. 135-151. Springer, Singapore, 2018.
15. Sagheer Ahmed and Amar Singh, Baddi University of Emerging Sciences and Technology Solan, Himachal Pradesh, "Literature Survey of MANETS Routing Protocols" International Journal of Technology and Computing (IJTC),Volume 2, Issue 7 July 2016, ISSN2455-099X
16. Opinder Singh, Dr. Jatinder Singh, and Dr. Ravinder Singh, IKG PTU, Kapurthala, Punjab, "Attacks in Mobile Ad Hoc Networks: A Survey" International Journal of Computer Science & Communication Networks, Volume 6(4),194197, August-September 2016.
17. A Arjuna Rao, K Sujatha, A Bhavana Deepthi and L V Rajesh, Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagram, India, "Survey paper comparing ECC with RSA, AES and Blowfish Algorithms" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 5 Issue: 1 January 2017 ISSN: 2321-8169.
18. Suman Bala, Er.Amandeep Singh Bhandari and Dr. Charanjit Singh, Department of Electronic & Communication Punjabi University, Patiala India, "A Survey on Various Routing Protocols in Manet with Various Protection Schemes" International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 6, June 2017,ISSN: 2321-8169.
19. Smriti Jain and Nakka Marline Joys Kumari, School of Information TechnologyVIT University, VelloreTamilnadu, India, "A Survey on Trust Based Secure Routing in MANET" International Journal of Research and Scientific Innovation (IJRSI), Volume 4, Issue 8, August 2017, ISSN 2321–2705.
20. D.Santhosh Kumar, Dr.K.Thirunadana Sikamani "Efficient And Secure Trust Based Ad Hoc Routing in MANET", International Conference on Current Trends in Engineering and Technology, ICCTET'13 .
21. Dilli Ravilla, Dr Chandra Shekar Reddy Putta "Performance of Secured Zone Routing Protocol due to the Effect of Malicious Nodes in MANETs", 2013 IEEE
22. Akshai Aggarwal "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs", 2014 Fourth International Conference on Advanced Computing & Communication Technologies.
23. Aida Ben Chehida Douss , Ryma Abassi , Sihem Guemara El Fatmi "A Trust Management based Security Mechanism against Collusion Attacks in a MANET Environment", 2014 9th International Conference on Availability, Reliability and Security .
24. Antesar M. Shabut, Keshav Dahal, Irfan Awan "Friendship Based Trust Model to secure routing protocols in Mobile Ad hoc Networks", 2014 International Conference on Future Internet of Things and Cloud.
25. David Airehrour, Jairo Gutierrez, Sayan Kumar Ray " GradeTrust: A Secure Trust Based Routing Protocol For MANETs", 2015 International Telecommunication Networks And Application Conference(ITNAC).
26. Mazda Salmanian and Ming Li "Enabling Secure and Reliable Policy-based Routing in MANETs", 2013 IEEE.
27. Harris Simaremare , abdelhafid abouissia, RIRI FITRI SARI,"performance analysis of optimized trust aodv using ant algorithm", IEEE ICC 2014 - Communications Software, Services and Multimedia Applications Symposium.
28. KefayatUllah, Rajib Das,Prodipto Das, Ananya Roy "Trusted and Secured Routing in MANET: An Improved Approach", 201 5 International Symposium on Advanced Computing and Communication (ISACC)
29. Saadoune M, Hajami A, Allali H (2014) Distance's quantification algorithm in AODV protocol. Int J Comput Sci Inform Technol 6(6):177–188
30. T. T. Son, H. L. Minh, G. Sexton and N. Aslam, A novel encounterbased metric for mobile ad-hoc networks routing, International Journal of Ad Hoc Networks, vol.14, pp. 2-14. March 2014.
31. R. Feng, S. Che, X. Wang, and N. Yu, " A Credible Routing Based on a Novel Trust Mechanism in Ad Hoc Networks" In International Journal of Distributed Sensor Networks, vol. 2013, Article ID 652051, 2013, 12 pages.
32. De Couto, D.S.J., Aguayo, D., Bicket, J., Morris, R., 2003. A high-throughput path metric for multi-hop wireless routing. In: ACM Proceedings of the 9th Annual International Conference on Mobile computing and Networking, New York, NY, USA
33. A.P. Dempster, A generalization of Bayesian inference, in: R.R. Yager, L. Liu (Eds.), Classic Works of the DempsterShafer Theory of Belief Functions, Springer-Verlag, Berlin, Germany, 2008, pp. 73104.