Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/110321

Proficient and Secured Routing in MANET Based on Trust and Energy Supported AODV

S. Sridhar[1,*], *R. Baskaran*[2], *R. Anitha*[3] *and R. Sankar*[3]

[1] Department of Computer Applications, S.A.Engineeing College, Chennai - 77, India
[2] Dept of Computer Sc. & Engg., CEG, Anna University, Chennai -25, India
[3] Dept. of Computer Applications, S.A.Engineering College, Chennai-77, India

Received: 13 Feb. 2017, Revised: 9 Mar. 2017, Accepted: 18 Mar. 2017
Published online: 1 May 2017

Abstract: A Mobile ad-hoc network (MANET) is a wireless network, self-configuring, quickly deployable and operates without infrastructure. More focus is towards MANET because of its realistic applications and necessity of communication in mobile devices. Nodes communicate between them without any centralized management and are movable since topology is very vibrant and they have restricted energy and computing resources. Dynamic nature of MANET demands end to end quality of service by upholding connectivity and providing reliable and consistent transmission. Secured transmission enhances the efficiency of real-time applications where MANET is used. Nodes trust and energy levels are to be considered for providing trustworthy transmission. The proposed protocol (TES-AODV) incorporates trust, energy and security management and nodes selected for routing based on its trust and energy values. A threshold value is defined and nodes are ideal for routing only if its trust and energy levels are superior to threshold. The transmissions are made secure by introducing message digest algorithm, MD5 which creates unique signatures for each node that take part in routing thus providing reliability of routing. The work is implemented and simulated on NS-2. The simulation results have shown a good improvement over the quality of service metrics like PDR, Delay, Throughput, Jitter and residual energy. Thus TES-AODV provides more consistent, reliable and secured data transfer compared to general AODV and DSR protocols.

Keywords: MANET, TES-AODV, Trust, Energy, MD5, PDR.

1 Introduction

Mobile Ad-Hoc network [1] is collection of wireless mobile nodes that self-organizes itself in dynamic network topologies. They do not rely on existing infrastructure to support communication among mobile nodes. Each mobile node acts as an end node when it is the source or destination of a communication and forwards packets for other nodes when it is an intermediate node of the route. Nodes can join and leave the network at anytime and are free to move arbitrarily and organize themselves randomly. The simplicity of deployment and the infrastructure less feature of Mobile Ad hoc Networks makes it extremely attractive for the present day scenarios. Ad hoc networks are easier to organize than wired networks and are used in many applications, such as in human or nature induced disasters, battlefields, meeting rooms. The dynamic nature of MANET makes it enormously complicated to obtain accurate knowledge of the network state and that's why the consistency of data transmission in this network cannot be guaranteed. Traditional routing protocols in MANET assume a collaborating environment inside the network. However, this suggestion is not always true and an aggressive or vulnerable environment can seriously affect network performance. MANET expects each participating node to forward packets.

This nature of MANET leads to the possibility that there could be some malicious nodes that makes MANET vulnerable.

Routing protocols in MANETs are generally classified as proactive and reactive [2]. Reactive routing protocols start to establish routes only when required or only if there is a demand. Some of the reactive routing protocols are AODV, DSR, TORA, ABR, SSA and RDMAR. The other classification of routing protocol is table-driven or pro-active routing protocols. Each node maintains one or more routing information table of all the

* Corresponding author e-mail: sridhar@saec.ac.in

participating nodes and updates their routing information regularly to maintain most up-to-date analysis of the network. Some of the proactive routing protocols are DSDV, WRP, CGSR and FSR.

In ensuring QoS provisioning, a network is expected to guarantee a set of measurable pre-specified service attributes to the users in terms of end-to-end performance, such as challenging task to ensure QoS provisioning including routing in ad-hoc networks due to the mobile and dynamic nature of the nodes. Recent QoS solutions are planned to operate on trusted environments and totally assume the participating nodes to be cooperative and well behaved. A few challenges faced in providing Qos are steadily changing environment, unobstructed mobility which causes recurring path breaks and also make the link-specific and state-specific information in the nodes to be inexact. Therefore, when it comes to QoS routing, the routing protocols have to ensure that the QoS requirements are met [3].

The idea of using trust to mitigate security threats has been an important area of research [4]. The concept of ”Trust” originally derives from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [5]. The trust based routing is one way to form cooperation among nodes for establishing an efficient routing between nodes. Trust value plays a crucial role in all of the network activities. Continuous evaluation of node’s performance is used to calculate the trust of this node. Basically Mobile ad hoc networks are designed for a cooperative environment but in hostile environments trust-based routing should be used. Instead of establishing the shortest routes as done in traditional routing protocols, trusted routes are established to make it a trustworthy routing.

MANETS usually consist of mobile battery operated devices that communicate over the wireless medium. These devices are battery operated and therefore need to be energy conserving so that the battery life of each individual node can be extended. Avoid nodes which have low energy [6]. To make the most of the lifetime of an ad hoc network, it is essential to lengthen each individual node life through minimizing the total transmission energy consumption for each communication request. Therefore, an efficient routing protocol must satisfy that the energy consumption rate at each node is evenly distributed and at the same time the total transmission energy for each request is minimized. If nodes which are highly trusted run out of energy then it is waste of putting in the overhead of calculating trust and then considering the node for routing. Therefore it is wise to select a node for efficient routing by considering its trust and energy values. The transaction made by nodes in MANET should be a secured transaction. To provide security for all transactions Message digest algorithm in introduced during transmission. All transmissions are secured using MD5 Algorithm. Thus it increases the reliability of routing

2 Literature Study

A reliable routing algorithm based on fuzzy logic [7] is proposed where three parameters are determined: trust value, energy value and reliability value which are used for finding a stable route from source to destination. During route discovery, every node records its trust value and energy capacity in RREQ packet. In the destination, based on reliability value, is decided which route is selected. The path with more reliability value is permitted to route data packets from source to destination. The proposed method has significant reliability improvement in comparison with AODV. An energy consumption model [8] to calculate the energy-factor of the nodes is considered and then a trust based protocol for energy-efficient routing is proposed. A trust module to track the value of routing metric is adopted. Simulation results show that the proposed protocol reduces delay, routing overhead, and increases packet delivery ratio by consuming less energy compared to AODV and DSR. Continuous evaluation of node’s performance and collection of neighbor node’s opinion value about the node are used to calculate the trust relationship of this node with other nodes.

A perfect trust model [9] is introduced in the network layer to establish secure route between source and destination without any intruders or malicious nodes. Thus the existing AODV routing protocol has been modified in order to adapt the trust based communication feature. Proposed trust based routing protocol equally concentrates both in node trust and route trust. Three-party password authenticated key exchange (3PAKE) protocols allow two clients to establish a common secure session key via the help of an authentication server, in which each client only needs to share a single password with the server. 3PAKE protocols are vulnerable to partition attacks and off-line dictionary attacks. A provably secure 3PAKE protocol [10] is proposed which is more efficient and secure than other related protocols.

A lightweight authentication scheme [11] is proposed that is designed to enable mobile devices to achieve robust client-anonymity and computation efficiency. Instead of the heavy encryption and decryption modules of Elliptic Curve Cryptography (ECC), we adopt the key agreement operation of ECC as the core technique in the proposed anonymous authentication scheme. This eliminates significant computation cost and thus does not exceed the inherent resource-limitations on mobile devices. Security analyses are conducted to guarantee the robustness of the proposed authentication scheme.

Strong designated verifier signature shows that only designated user can verify the validity of the signature, others who have not signer’s secret key or verifier’s secret key cannot judge the signature’s originator. A new strong designated verifier signature scheme [12] with time limit is proposed where, the message and time stamp need not transmit publicly, which were embedded in signature via

the method of message recovery, only singer and designated verifier can recover these secrete values. Based on the Bilinear Diffie-Hellman problem and Pre-Image Resistance assumption, it is proved that our new strong designated verifier signature scheme can resist the ordinary forgery attack and replay attack, and enforce signature verification with time limit.

A novel application-based model as a suitable alternative for the classification and identification of attacks on a computer network, and thus guarantee its safety from HTTP protocol-based malicious commands is proposed. The proposed model [13] is built on a self-recurrent neural network based on wavelets architecture with multidimensional radialwavelons, and is therefore suited to work online by analyzing non-linear patterns in real time to self-adjust to changes in its input environment. The results confirm that recurrent architectures using wavelets obtain superior performance than their peers, in terms not only of the identification and classification of attacks, but also the speed of convergence.

A modified AODV routing protocol called MAODV [14] is presented, which takes route stability into consideration to attempt to establish a more stable path between the source and destination. Some changes in Hello and RREQ message format are made to respectively record the sending time and route stability factor. MAODV shows a better performance. A power-aware ad hoc on-demand distance vector routing protocol (PAW-AODV) is proposed and investigated for efficient power routing [15]. PAW-AODV could use the limited power resources efficiently as it routes based on a power-based cost function. Both AODV and PAW-AODV are simulated in various mobile situations and are also subjected to the various hop count limits that the data could traverse from source to destination. Their performances in the various scenarios are then compared to reflect the relative merits of each protocol.

A routing algorithm [16] which adds a field in request packet which stores trust value indicating node trust on neighbor is proposed. Based on level of trust factor, the routing information will be transmitted depending upon highest trust value among all. This not only saves the node's power by avoiding unnecessary transmitting control information but also in terms of bandwidth (channel utilization), which is very important in case of MANET. The malicious node can attack on the control packet and misbehave in the network. The malicious node, which may or may not be trusted node. Here, a trusted path irrespective of shortest or longest path which can be used for communication in the network is proposed. Route trust value is calculated on the complete reply path which can be utilized by source node for next forthcoming communication in the network. A security-enhanced AODV routing protocol [17] called R-AODV (Reliant Ad hoc On-demand Distance Vector Routing) is presented. The implementation is done by a modified trust mechanism known as direct and recommendations trust model and then incorporating it inside AODV which will allow AODV to not just find the shortest path, but instead to find a short path that can be trusted. This enhances security by ensuring that data does not go through malicious nodes that have been known to misbehave. The R-AODV protocol does provide a more reliable data transfer compared to the normal AODV if there are malicious nodes in the MANET.

Two kinds of approaches [18] are applied to a well-known routing protocol called SAODV in order to improve its performance and to offer more resilience to attack from malicious nodes authenticated by the network. A preventive approach based on a cryptographic mechanism and a reactive approach to detect the anomalous and malicious behavior of nodes is considered. An extension of SAODV to offer Intrusion Detection mechanism (IDM) and trust-based mechanism (TBM) to promote the collaboration of the cooperating node and penalize the selfish nodes are proposed. The extended and proposed protocol SAODV-SDO is presented and simulation results performed in order to show the effectiveness of the proposed protocol in comparison with AODV and SAODV.

3 Methodology

It is tough to provide reliable and efficient routing in routing in mobile ad hoc networks because of its dynamic nature that keeps nodes moving and not stable. In spite of this nature nodes communicate with each other and exchange data among the nodes that are in its range on the network. But still there are nodes in the MANET which take part in routing but drop packets while transmitting packets which affects the performance of the protocol. Nodes should also have sufficient energy to perform transmission successfully. A trust and energy based AODV [19] is introduced which provides reliable nodes with sufficient energy levels for routing.

3.1 Trust Calculation

In the MANET, an observation is made on all nodes that transmit packets. The total packets they transmit, packets they receive and the packets they drop are taken in to account for trust value calculation. The trust level value calculation is based on the parameters shown in the Table 1. The count field describes about two criteria success and failure which describes whether the transmission was a successful transmission or a failure

Table 1 Node Trust calculation parameters

Count Type	RREQ	RREP	Data
Success	Qrs	Qps	Qds
Failure	Qrf	Qpf	Qdf

RREQ and RREP are the route request and route reply respectively which are exchanged between nodes in the network. Data refers to the payload transmitted by the nodes. The parameter Qrs is defined as the query request success rate which is calculated based on number of neighboring nodes who have successfully received (rreq) from the source node which has broadcasted it, Qrf defined as the query request failure rate which is calculated based on number of neighboring nodes which have not received the query request.

Qps is defined as the query reply success rate which is calculated as successful replies (rrep) received by the source node which has sent the rreq and Qpf is defined as the query reply failure rate which is calculated based on the number of neighboring nodes which have not sent the replies for the query request received. Qds is defined as the data success rate calculated based on successfully transmitted data and qdf is defined as data failure rate calculated based on data which have failed to reach destination. However, it is known that for every network there will be minimum data loss due to various constraints.

Qr, Qp and Qd are intermediate values that are used to calculate the nodes Request rate, Reply rate and Data transmission rate. The values of Qr, Qp, and Qd are normalized to fall in range of -1 to +1. If the values fall beyond the normalized range then it clearly shows that the failure rate of the node is high and denotes that the corresponding node may not be suitable for routing. Apart from the above mentioned normalized range, trust level value (TL) is calculated for each node during routing and is checked against the threshold (TT) value (Calculated by the average of trust values of the nodes that take part in the routing). If lesser than threshold then there is a possibility for this node to drop packets for the current transmission and will not be suitable for routing and an alternate path is selected for routing. However, this node may be the best node for some other transmission between some other source and destination in the same network at different time interval.

The next hop node is selected based on the trust value. To select the next hop node the trust value of all neighboring nodes from current source node is calculated and finally a node which has highest value than the threshold is selected as next hop node for the current routing. For example, Route starts from node N1 and next hop node N2 is selected. Now to select next hop node for N2 its neighbors are identified and their trust values are calculated. If N3, N4, N5, N6, N7 are the neighboring nodes of N2 then trust value for all these nodes are collected and an average of this is identified and this value is set as threshold value for selecting the next hop node for N2 only. The node which has the highest trust value than the threshold will be selected as next hop node. Threshold value is calculated dynamically for every next hop node selection in each run. The nodes which are not selected for the current transmission based on their trust value cannot be tagged as unfit node because it can serve as best trusted node for another transmission based on the scenario. Therefore based on the above calculation the following two cases are derived based on the threshold value.

Case 1: The node's trust value is checked with the threshold value and if the value is greater than the threshold value then the node is defined a trustworthy node and is allowed to participate in routing thereby assuring a trustworthy routing in MANET.

Case 2: If the nodes trust value is less than or equal to threshold value then the node in defines as untrustworthy node which cannot be allowed to participate in routing which causes packet dropping. In both cases the trust calculation is performed regularly to check the nodes performance and help it to be marked trustworthy or not.

3.1.1 Trust calculation Procedure

Step1. Begin For nodes i to n do.

Step2. Initialize qrs, qps and qds //Success rate parameters.

Step3. Initialize qrf, qpf and qdf //Failure rate parameters

Step4. Initialize QR, QP and QD // Intermediate values of request, reply and date respectively.

Step5. Calculate QR : $QR = \sum_{i}^{n} \frac{qrs - qrf}{qrs + qrf}$

Step6. Calculate QP : $QP = \sum_{i}^{n} \frac{qps - qpf}{qps + qpf}$

Step7. Calculate QD : $QD = \sum_{i}^{n} \frac{qds - qdf}{qds + qdf}$

Step8. Calculate Trust Level Value:

$TL = T(RREQ) * QR + T(RREP) * QP + T(DATA) * QD$

//T is the time factorial of RREQ, RREP, DATA sent respectively

Step9. For all neighbor nodes j to n do

Step10. Calculate Trust-Threshold: $TT = \sum_{i}^{n} \frac{TL}{n}$

Step11. End

3.2 Energy Calculation

In MANET, nodes energy also plays a key role. Node should have a good energy level to complete the transmission successfully. Though the node is said to be a reliable node and has a good success rate of transmission, it fails if it does not have energy. Therefore energy becomes vital for all nodes to perform a efficient

transmission. A node is selected for routing only if its energy level is greater than the threshold value (average of energy values of the neighboring nodes). Energy calculation is based on nodes transmission, reception, idle and overhears modes. To identify energy level the nodes are evaluated where sender to increase radio frequencies to identify best nodes with more energy levels. Current Energy level of node can be calculated by the initial energy level and the consumed energy level of a node. For every transmission the transmission power and reception power gets subtracted from its initial value of 100 Joules (initialized during simulation).

During simulation communication messages (RREQ and RREP) are exchanged between nodes in the network. RREP contains energy values also. Therefore, energy for nodes needs to be considered while routing since nodes may drain out of energy levels. Though a node is providing its complete support for routing it can perform well only if it has sufficient energy. Thus, energy is announced by the proposed AODV protocol that checks for energy levels of nodes before taking part in routing to make the MANET routing efficient and effective and also ensure QoS.

3.2.1 Energy value calculation procedure

Step1. Do For all intermediate nodes which receive request from a source node.

Step2. Introduce energy for all nodes and set initial parameters values as initial-energy = 100, max-energy=100, nodes=50 and Node-id (unique id for each node)

Step3. Calculate Intermed-energy based on event, time where events can be (event = ”Tm” || event= ”Rm” || event=”Om”|| event=”Im”) //Transmit mode, Receive mode, Overhear mode and Idle mode.

Step4. Every node in the MANET calculates its power consumption and finds the remaining energy periodically. Each node may operate in any of the following modes;

Step4a. In Transmission mode, the power consumed for transmitting a packet is given as

Consumed-energy $= Pt * T$

Where Pt is the transmitting power and T is the transmission time.

Step4b. In Reception mode, the power consumed for receiving a packet is given as

Consumed-energy = Pr * T

Where Pr is the reception power and T is the reception time.

Step4c. In Idle mode, the power consumed in idle mode is given as

Consumed-energy = Pi * T

Where Pi is the power consumed in idle mode and T is the idle time.

Step4d. In Overhear mode, the power consumed in overhearing is given as

Consumed-energy = Po * T

Where Po is the power consumed in overhearing and T is overhear time.

Step4e. Calculation of consumed-energy and total-energy;

for (i in Intermed-nergy)

{Consumed-energy[i]=initial-energy-Intermed-energy[i]

Total-energy +=consumed-energy[i]

if(max-energy¡consumed-energy[i])

{Max-energy=consumed-energy[i]

Node-id=i}}

Step5. The value T (time) can be calculated as

T= Data size / Data rate

Step6. Hence, the remaining energy of each node can be calculated as;

Rem-energy = Current-energy - Consumed-energy

Step7. Node which sends route request collects energy value of all nodes which receive the request from source and reply to source along with their energy value (consumed energy).

Step8. Compute threshold as total energy of nodes replied to node that has sent request by number of nodes replied. Calculate

Energy-Threshold $ET = \sum_{i}^{n} \frac{\text{Consumed energy}}{n}$

Step9. Next hop node selected based on its energy value which is higher than ET.

Step10. Compute average energy:

Average-energy = total - energy / nodes

Initially every node has full battery capacity say 100% which is assigned to current energy .On each event, the remaining energy is calculated. A threshold (ET) is set where the average Rem-energy of all nodes that are eligible for next hop is calculated and the node which has

got Rem-energy value more than the threshold is selected as next hop node.

3.3 Secured transmission using MD5

The critical job in routing is to identify the attackers in the path. To identify the attackers we initially set (flag) all nodes as true nodes. Nodes change their nature only after performing transmissions. Nodes properties considered are IP Address (IP), Nodes identification (ID), MAC Address and msg. If any one of these property of a node is altered or changed, we conclude the node is an attacker [30]. We propose that change in ip address concludes the node as attacker. Initially ip is set in a sequence. Example set ip_node0 192.26.2.0; set ip_node1 192.26.2.1; set ip_node2 192.26.2.2; set ip_node3 192.26.2.3; set ip_node4 192.26.2.4; set ip_node5 192.26.2.5.

If any node uses a another ip which is already existing then we conclude that node as attacker. Ip address are set in sequence. For instance node 5 and node 10 has same ip address, then check node's flag whether its true or false. It would be true for node 5 but false for node 10 since the ip is replicating for node 10. Since we have set ip addresses in sequence its clear that the current ip address of node originally belongs to node 5. These algorithms operate on a message 512 bit at a time. Pad the msg to a multiple of 512 bits. Digest calculation begins with digest value initialized to a constant. This value is combined with first 512 bits of msg to produce a new value for the digest; using a complex transformation. New value is combined with next 512 bits of msg using same transformation and so on until final value of digest is produced. The main ingredient of MD5 alg is the transformation that takes input as current value of the 128 bit digest, plus 512 bits of msg and outputs a new 128-bit digest. MD5 operates on 32 bit quantities. Current digest value can be thought of as four 32-bit words(d0, d1, d2, d3) and piece of msg currently being digested (512) as sixteen 32 bit words (M0 through M_{15}).

Step 1: We create a matrix for random values to be selected. We take a 4x4 matrix to increase the combination and possibilities as shown below.

0*xd*76*aa*4780*xe*8*c*7*b*7560*x*242070*db*0*xc*1*bdceee*
0*xf*57*c*0*faf*0*x*4787*c*62*a*0*xa*83046130*xfd*469501
0*x*698098*d*80*x*8*b*44*f*7*af*0*xffff*5*bb*10*x*895*cd*7*be*
0*x*6*b*9011220*xfd*9871930*xa*679438*e*0*x*49*b*40821

0*xf*61*e*25620*xc*040*b*3400*x*265*e*5*a*510*xe*9*b*6*c*7*aa*
0*xd*62*f*105*d*0*x*24414530*xd*8*a*1*e*6810*xe*7*d*3*fbc*8
0*x*21*e*1*cde*60*xc*33707*d*60*xf*4*d*50*d*870*x*455*a*14*ed*
0*xa*9*e*3*e*9050*xfcefa*3*f*80*x*676*f*02*d*90*x*8*d*2*a*4*c*8*a*
0*xffffa*39420*x*8771*f*6810*x*6*d*9*d*61220*xfde*5380*c*
0*xa*4*beea*440*x*4*bdecfa*90*xf*6*bb*4*b*600*xbebfbc*70
0*x*289*b*7*ec*60*xeaa*127*fa*0*xd*4*ef*30850*x*4881*d*05
0*xd*9*d*4*d*0390*xe*6*db*99*e*50*x*1*fa*27*cf*80*xc*4*ac*5665

0*xf*42922440*x*432*affff*970*xab*9423*a*70*xfc*93*a*039
0*x*655*b*59*c*30*x*8*f*0*ccc*920*xffeff*47*d*0*x*85845*dd*1
0*x*6*fa*87*e*4*f*0*xfe*2*ce*6*e*00*xa*30143140*x*4*e*0811*a*1
0*xf*7537*e*820*xbd*3*af*2350*x*2*ad*7*d*2*bb*0*xeb*81*d*391

Step 2: The format define how message should take values from matrix and in what format. For example if null then first option, if 'a' then second option and this goes on. It should be in a combination alphabets, numbers and alphanumeric characters. Even if there no messages to be transmitted there should be a 32 bit message.

For each {msg expected}
{
""
"*d*41*d*8*cd*98*f*00*b*204*e*9800998*ecf*8427*e*"
"*a*"
"0*cc*175*b*9*c*0*f*1*b*6*a*831*c*399*e*269772661"
"*abc*"
"900150983*cd*24*fb*0*d*6963*f*7*d*28*e*17*f*72"
"*abcdefghijklmnopqrstuvwxyz*"
"*c*3*fcd*3*d*76192*e*4007*dfb*496*cca*67*e*13*b*"
}
This 32 bit consumes more time for an attacker to decrypt.

Step 3: Is expected and computed are same? If same we conclude message formed as per the following. Expected is the output of step 2, that is the message created as per the format defined above. Computed is the message created following the formats defined and applied to md5 algorithm.

```
puts "testing: md5 ¨$msg¨"
set computed [md5 $msg]
puts "expected: $expected"
puts "computed: $computed"
if {0 != [string compare $computed
$expected ] }
{
puts "FAILED"
}else
```

```
{
   puts ”SUCCEEDED”
   }
```

4 Experimental results

Trust, energy and security schemes are applied to the network scenario with different range of nodes. The same scenario is applied for traditional AODV and DSR. This helps the data packets to favourably move towards the destination by using trusted and energy efficient paths. The wireless network of this work comprises of 25, 50 and 100 nodes. The simulation results obtained from the execution of TES-AODV is compared with the simulation results obtained from the execution of traditional protocols like AODV and DSR. Results are compared in terms of Packet delivery ratio, Throughput, Delay, Packet loss and residual energy. The proposed TES-AODV shows good improvement in Qos metrics. PDR and Throughput are higher, delay and packet loss are reduced and energy consumption is also less compared with general AODV and DSR. The experiments results were obtained against different number of nodes and different pause time. The results shows an average of 20% increase in PDR. This increase is because nodes are selected based on their trust and energy value. The next hop node selected to complete the path form source to destination, is based on its trust and energy value. This trust and energy based routing assures an efficient routing and avoids misbehaving nodes in routing path. The proposed TES-AODV has also shown a decreased delay and an increase in throughput. Nodes which are trusted and with high energy levels are alone used for routing which ultimately reduces the time taken to reach the destination successfully. Energy is vital for a node to perform in the network. Nodes with good trust may be selected for routing but inefficient energy may lead to poor performance of the node towards routing. This scheme selects node for only routing which has good energy values. The energy consumption of nodes is reduced so that they maintain good energy levels for future transmission and extend their lifetime in the network.

4.1 Results comparison of QoS metrics with respect to node count and pause time

Qos parameters are discussed in the following sections to show the enhancements in proposed TES-AODV protocol compared to general AODV and DSR.

4.1.1 Packet Delivery Ratio

As shown in Fig. 1. and Fig. 2., TES-AODV outperforms AODV and DSR. The factor that contributes to the success of TES-AODV is the routing path that is established only with trustworthy and energy efficient nodes which are highly reliable and thus guarantees routing by eliminating misbehaving nodes in the routing path and providing higher packet delivery compared with AODV and DSR.

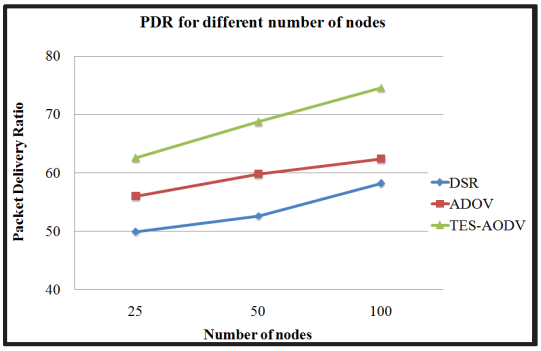

Figure 1 PDR for different nodes

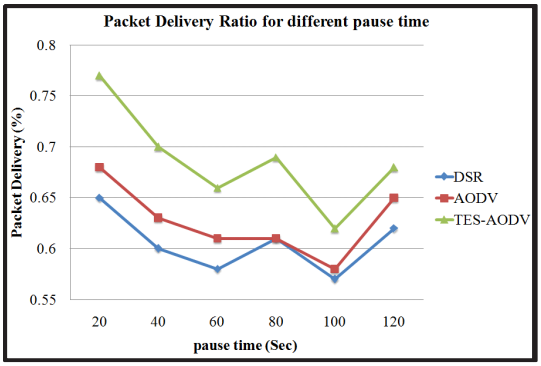

Figure 2 PDR for different Pause time

4.1.2 Throughput

TES-AODV is on middling 30% better than AODV and 35% better than DSR in terms of middling throughput as shown in Fig. 3 and Fig.4. Since the possibility of finding an reliable and efficient route for TES-AODV is higher than that of AODV and DSR

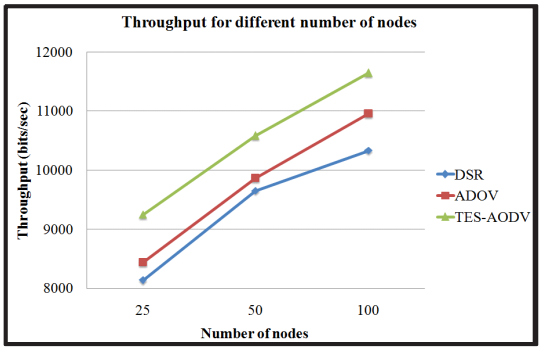

Figure 3 Throughput for different nodes

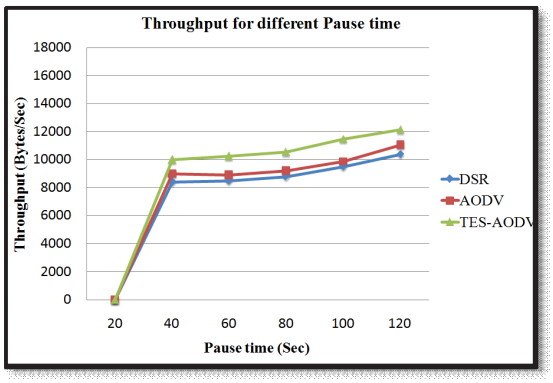

Figure 4 Throughput for different Pause time

4.1.3 Packet Drop

As an attractive asset lesser number of packets should be dropped while communication. Fig. 5. and Fig. 6. indicate that TES-AODV is better than AODV and DSR. The proposed TES-AODV creates efficient routes there by reducing the packet drop in the routing path. TES-AODV drops fewer packets compared to AODV and DSR.

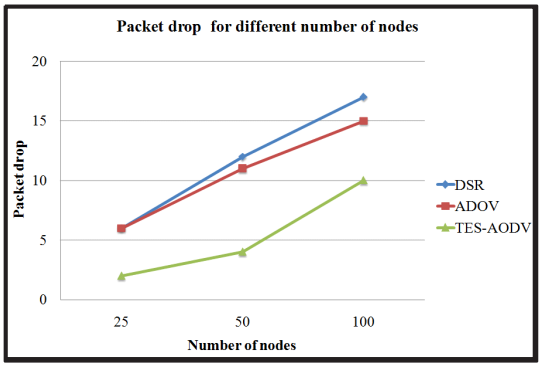

Figure 5 Packet drop for different nodes

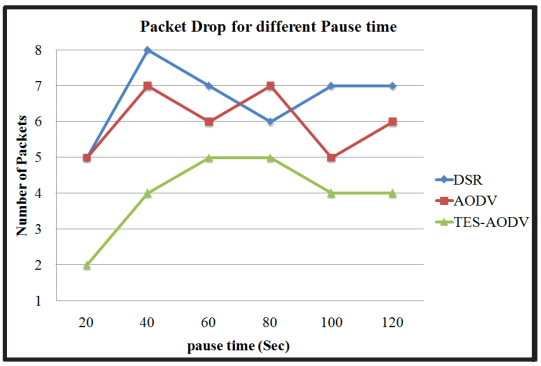

Figure 6 Packet drop for different Pause time

4.1.4 Delay

Despite enhanced performance of TES-AODV in terms of packet delivery ratio and throughput, TES-AODV outperforms AODV in delay as shown in Fig.7. and Fig. 8. The key reason for this is the trust and energy calculation to be carried out by TES-AODV at different pause time. Still TES-AODV delay is less than AODV and always better than DSR.

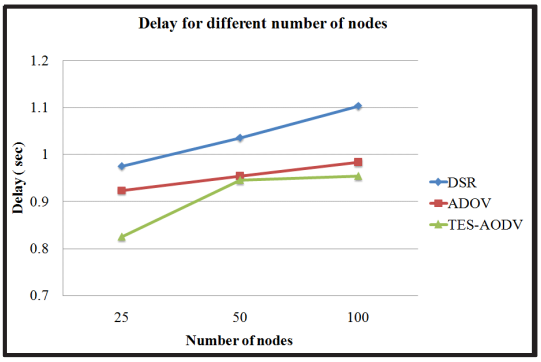

Figure 7 Delay for different nodes

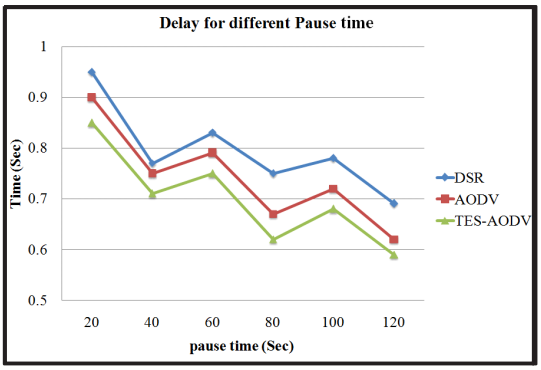

Figure 8 Delay for different Pause time

4.1.5 Jitter and Residual energy

Fig. 9. clears shows that the jitter for TES-AODV is less than AODV and DSR with respect to pause time. Fig. 10 depicts the energy remaining by different protocols at different pause times. TES-AODV consumes less energy compared to DSR and AODV.

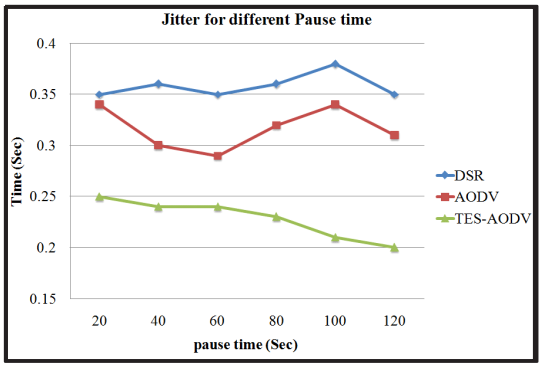

Figure 9 Jitter for different Pause time

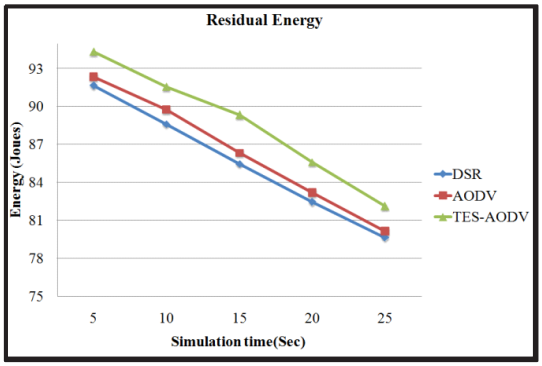

Figure 10 Residual energy

4.2 Security Scheme scenarios

The simulation snapshots of network are shown in Fig. 11. and Fig. 12.The nodes are marked initially as true and as transmission starts they start changing.

Flag for node(1)$---->$ true
Flag for node(2)$---->$true
Flag for node(9)$---->$ flase
Flag for node(28)$---->$flase

Routing Path : N23, N1, N40, N41, N48
Mis-behaving Routing : N23, N9, N28, N48
Alternative Routing :N23, N1, N2, N40, N41,N48
Mis-behaving Nodes : Node 9, Node 28

If node is replicating the ip address of another node then same msg to be created for both nodes by MD5. Hence both nodes will be tested with their flags where node 1 and 2 will be true and node 9 and 28 will be false. Node 9 and 28 are defined as attackers since they replicate ip address shown clearly with same msg been created using MD5. Table 2 depicts the signature of nodes used during routing.

Table 2 Signature of nodes

Routing Node	Signature
N1	c4dfd145e649849eb4a66f83c052a8de
	- Trusted Node
N9	c4dfd145e649849eb4a66f83c052a8de
	- Replicated as N1
N28	a9913d1a1eaccaa08606200dc92faaac
	- Replicated as N2
N2	a9913d1a1eaccaa08606200dc92faaac
	- Trusted Node

The snapshots show clearly that nodes are always checked for their reliability. If a node misbehave or becomes attacker immediately its been identified and an alternate routing path is established which ensures secured routing in proposed MANET routing.

5 Conclusion

A trust and energy based $AODV(TES-OADV)$ protocol is proposed that incorporates trust values, energy values of nodes and security management in $MANET$. Nodes are selected for routing based on its trust and energy values. A threshold value is defined and nodes are ultimate for routing only if its trust and energy levels are better than threshold. The transmissions are secured by implementing message digest algorithm MD5, which increases the reliability of routing. The work is implemented and simulated on NS-2 toward number of nodes and pause time. The simulation results have shown an good improvement over the qos metrics like PDR, Delay, Throughput, Jitter and residual energy. PDR increased by 24%, Throughput by 30%, Delay decreased by 6% and Packet loss reduced by 9%. Thus TES-AODV provides more consistent, reliable and secured data transfer compared to general AODV and DSR protocols. The work can be implemented and compared with other reactive and proactive protocols and also can implement virtual energy concepts for increasing the efficiency of proposed protocol.

References

[1] G. Kortuem, J. Schneider, D. Preuitt, T.G.C. Thompson, S. F'ickas, Z. Segall. When Peer to-Peer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad

hoc Networks. First International Conference on Peer-to-Peer Computing, August, Linkoping, Sweden, pp. 75-91, 2001.
[2] Remondo. Tutorial on wireless ad hoc networks. Second International Conference in Performance Modeling and Evaluation of heterogeneous networks, July 2004.
[3] I. Jawhar, and J. Wu. Quality of Service Routing in Mobile Ad Hoc Networks. In: M Cardei, I Cardei & DZ Du (eds), Resource Management and Wireless Networking, Kluwer Academic Publishers.
[4] T. Beth, M. Borcherding and B. Klein. Valuation of trust in open networks. Proceedings of ESORICS 1994, November 1994.
[5] K. S. Cook. Trust in Society. vol. 2, Feb. 2003, Russell Sage Foundation Series on Trust, New York.
[6] K. Muthumayil, V. Rajamani, S. Manikandan. A novel cross layered energy based ad hoc on-demand routing protocol for MANETs. Proceedings of Third International Conference on Advanced Computing (ICoAC), pp. 276-281, 2011.
[7] Arash Dana, Golnoosh Ghalavand, Azadeh Ghalavand, Fardad Farokhi. A Reliable routing algorithm for Mobile Adhoc Networks based on fuzzy logic. In: International Journal of Computer Science Issues, vol.**8**, issue 3, no. 1, pp. 128 - 133, 2011.
[8] S. Sarkar, R. Datta. A trust based protocol for energy-efficient routing in self-organized MANETs. Annual IEEE India Conference (INDICON), pp. 1084 - 1089, 2012.
[9] A.M. Pushpa. Trust based secure routing in AODV routing protocol. IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA), pp. 1 - 6, 2009.
[10] Wei FuShan, Ma Jianfeng, Ge Aijun, Li Guangsong, Ma Chuangui. A Provably Secure Three-Party Password Authenticated Key Exchange Protocol without Using Server's Public-Keys and Symmetric Cryptosystems. In: Information technology and control, vol.**44**, no.2, pp. 195 - 206, 2015.
[11] Kuo-Hui Yeh. An Anonymous and Lightweight Authentication Scheme for Mobile Devices. In: Information technology and control, vol 44, no.2, pp. 206- 215, 2015.
[12] Yulei Zhang, Yongjie Zhang, Yahong Li, Caifen Wang. Strong Designated Verifier Signature Scheme Resisting Replay Attack. In: Information technology and control, vol. **44**, no.2, pp. 165 - 171, 2015.
[13] V. Alarcon-Aquino, J. M. Ramirez-Cortes, P. Gomez-Gil, O. Starostenko, Y. Garcia-Gonzalez. Network Intrusion Detection Using Self-Recurrent Wavelet Neural Network with Multidimensional Radial Wavelons. In: Information technology and control, vol. **43**, no.4, pp. 347 - 358, 2014.
[14] Mou Zonghua , Meng Xiaojing. A modified AODV routing protocol based on route stability in MANET. Fourth IET International Conference on Wireless, Mobile & Multimedia Networks, pp. 63 - 67, 2011.
[15] Chee-Wah Tan , S.K. Bose. Investigating Power Aware AODV for Efficient Power Routing in MANETs. Fifth International Conference on Information, Communications and Signal Processing, pp. 584 - 588, 2005.
[16] R.S. Mangrulkar, M. Atique. Trust based secured adhoc On demand Distance VectorRouting protocol for mobile adhoc network. Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), pp. 1 - 4, 2010.
[17] H.S. Jassim, S. Yussof, Tiong Sieh Kiong, S.P. Koh, R.A. Ismail. A routing protocol based on trusted and shortest path selection for mobile ad hoc network. Ninth Malaysia International Conference on Communications (MICC), pp. 547 - 554. 2009.
[18] F. De Rango. Improving SAODV protocol with trust levels management, IDM and incentive cooperation in MANET. Wireless Telecommunications Symposium, 2009, pp. 1 - 8.
[19] Sridhar and Baskaran. Efficient Routing in Mobile Adhoc Networks Emphasizing Quality of Service by Trust & Energy based AODV. In: Journal of Communications Software and Systems, vol. **11**, no. 1, pp. 1-7, 2015.
[20] Sridhar and Baskaran. Secured and Energy based QoS routing in MANETs. In: The International Journal of Computer Science and Business Informatics, vol. **1**, no. 1,, pp.11-13, 2013.

S. SRIDHAR received UG degree, B.Sc. Computer Science from the University of Madras, Chennai, India, in 1998, PG degree, Master of Computer Applications (MCA) from University of Madras, Chennai, India, in 2001 and another PG degree Master of Philosophy (M.Phil.) in Computer Science from Periyar University, Salem, Tamil Nadu, India, in 2007. Awaiting for final Viva Voce for Ph.D. degree in computer science at Barathiyar University, Coimbatore, Tamil Nadu, India. Since 2001 he has been working with Department of Computer Applications (MCA), S.A.Engineering College, Chennai, India and currently heading the department. Has got more than 18 international publications. Research interests include Mobile Adhoc networks, Wireless sensor networks and Adhoc networks. Editorial member of 4 International Journals and reviewed many technical papers for conferences and journals.

R. BASKARAN obtained M.E. and Ph.D. in the field of Computer Science and Engineering in Anna University at Chennai, India. Currently working as Associate professor in Department of computer science, Anna University, Chennai India. Has a decade of experience as an academician and his research areas include Multimedia and principles, Software quality engineering, Software Agents and Distributed networking. Has published around 110 research papers in National and International Journals and Conferences. He is a member of various forums. He is the editor and a

reviewer of various journals. He is guiding research scholars working in area of software standards for Attributes Specific SDLC Models & Evaluation and Metric Based Efficient Traffic .

R. Anitha, received UG degree B.Com. in 2000 and PG degree Master of Computer Applications in 2000 from the University of Madras, Chennai, India. Completed Master of Philosophy (M.Phil) in Computer Science from Vinakya Mission, Chennai, India in 2009 and Master of Technology (M.Tech) in Computer Science from SRM University, Chennai, India, in 2013. She has been working with Department of Computer Applications (MCA) in S.A. Engineering College,Chennai, India since 2006. Has got 4 international publications and research interest includes Wireless Sensor Networks, Mobile Adhoc Networks and BigData.

R. Sankar received UG degree, B.Sc., Mathematics from the University of Madras, Chennai, India, in 2007 and PG degree, Master of Computer Applications (MCA) from Anna University, Chennai, India in 2010. He has been working with Department of Computer Applications (MCA) in S.A. Engineering College, Chennai since 2011. Has got 2 international publications and research interest includes Wireless Sensor Networks, Mobile Adhoc Networks, neural Networks.