A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks

Gautam M. Borkar[1] · A. R. Mahajan[2]

Published online: 24 May 2016

Abstract A mobile ad hoc network (MANET) is a self-configurable network connected by wireless links. This type of network is only suitable for provisional communication links as it is infrastructure-less and there is no centralized control. Providing QoS and security aware routing is a challenging task in this type of network due to dynamic topology and limited resources. The main purpose of secure and trust based on-demand multipath routing is to find trust based secure route from source to destination which will satisfy two or more end to end QoS constraints. In this paper, the standard ad hoc on-demand multi-path distance vector protocol is extended as the base routing protocol to evaluate this model. The proposed mesh based multipath routing scheme to discover all possible secure paths using secure adjacent position trust verification protocol and better link optimal path find by the Dolphin Echolocation Algorithm for efficient communication in MANET. The performance analysis and numerical results show that our proposed routing protocol produces better packet delivery ratio, reduced packet delay, reduced overheads and provide security against vulnerabilities and attacks.

Keywords Mobile ad hoc network (MANET) · Multicast routing scheme (MRS) · Quality of service (QoS) · AOMDV–SAPTV (ad hoc on-demand multicast distance vector–secure adjacent position trust verification) · Dolphin Echolocation Algorithm (DEA)

✉ Gautam M. Borkar
gautammborkar@gmail.com

[1] Rajiv Gandhi Institute of Technology, Versova, Andheri West, Mumbai, Maharashtra 400053, India

[2] Department of Information Technology, Government Polytechnic College, Nagpur, Maharashtra 440001, India

1 Introduction

A mobile ad hoc network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internet worked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension [1]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges [2, 3]; whereas nodes that not in the direct communication range use intermediate nodes to communicate with each other [4]. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network [5]. Routing protocols for ad hoc networks must deal with limitations such as high error rates, scalability, security, quality of service, energy efficiency, multicast, aggregation and node cooperation etc. [6]. Here, qualitative properties like security and quality of service are taken into account.

While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multi hop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment [7]. A MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to watch network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions

[8]. The primary goal of a MANET routing protocol is to establish a correct and efficient route between a pair of nodes so that messages may be delivered in a timely manner. If routing can be misdirected, the entire network can be paralyzed. Thus routing security plays an important role in the security of the whole network [9].

Quality of service (QoS) is usually defined as a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination [10]. QoS routing requires not only finding a route from a source to a destination, but a route that satisfies the end to-end QoS requirement, in terms of bandwidth or delay. The role of a QoS routing strategy is to compute paths that are suitable for different type of traffic generated by various applications while maximizing the utilizations of network resources. To find a path from source to destination satisfying user's requirements, to optimize network resource usage and to degrade the network performance when unwanted things like congestion, path breaks appear in the network [11] are the main objectives of QoS.

Routing is critical to QoS support, while its performance is vulnerable to changes in network topologies. In mobile wireless networks, such changes are mainly caused by node mobility [12]. Also security can be considered a QoS attribute. Without adequate security, unauthorized access and usage may violate QoS negotiations. The nature of broadcasts in wireless networks potentially results in more security exposure [10]. The physical medium of communication is inherently insecure, so we need to design security-aware routing algorithms for MANETs. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection across the entire protocol stack [13]. Owing to the fact that traditional routing protocols are not suitable for the unique characteristic of MANETs, a large number of research activities [14–26] have been carried out to explore and overcome the constraints of MANETs and solve design and application issues. The proposed multipath routing scheme (MRS) finds stable multicast path for multimedia transmission in MANET. A multipath mesh is constructed and the transmission route will discover in two stages. In first stage to maintain the quality of routing the physical parameter analysis will done by analyzing Transmit Energy, Distance, channel load, buffer occupancy, bandwidth and bit error rate (BER). Then in second stage the security of route will be analyzed by using route request and route reply packets. One of the most stable paths with better quality for routing in the secure environment is discovered by employing Dolphin Echolocation Algorithm (DEA) technique. Then the Route maintenance will process to maintain the routing in case of any link failure happened. The proposed scheme is simulated over a large number of MANET nodes with wide range of mobility and the performance is evaluated. The performance of the proposed scheme is compared with the existing routing protocols.

The main technical contributions of our work are summarized as follows:

1. We firstly give the definition and derivation of trust, then abstract a multipath routing model, where the trust an entity has for an interest neighbor forms the basic building block of this model. Basing on the interest entity's historical behaviors, multi-dimensional trust attributes are incorporated to reflect trust relationship's complexity in various angles.
2. The standard ad hoc on-demand multi-path distance vector protocol (AOMDV) is extended as the base routing protocol to evaluate the proposed secure and trust based multipath routing model. In the secure and trust based multipath routing scheme, Hop Count, Secure Forward Path Trust and Secure Reverse Path Trust, the three metrics compose a three-dimensional evaluation vector for routing decision and DE (Dolphin Echolocation) Algorithm provide a flexible and feasible route selection to establish multiple two-way trusted paths without containing the untrustworthy entities instead of the shortest route.
3. The performance evaluation show that the proposed multipath routing scheme provides better in attack prevention and makes a development on the packets delivery ratio, routing packets overhead, route discovery frequency and intrusion detection.

The remaining paper is organized as follows. Section 2 discusses the literature work. In Sect. 3, we describe our secure adjacent position trust verification model in detail. Basing on the proposed AOMDV–SAPTV routing protocol, in Sect. 4, the parametric matrices analysis and experimental results of AOMDV–SAPTV is given. Finally, Sect. 5 gives the concluding remarks of this paper.

2 Related work

Paramasivan et al. [27] have used the dynamic Bayesian signaling game to analyze the strategy profile for regular and malicious nodes in MANET for Routing. This game also revealed the best actions of individual strategies for each node. Perfect Bayesian equilibrium (PBE) provides a prominent solution for signaling games to solve incomplete information by combining strategies and payoff of players that constitute equilibrium. This game can also furnish secure and reliable communication that makes effective cooperation among nodes. Using PBE strategies of nodes are private information of regular and malicious nodes. Regular nodes should be cooperative during routing and update their payoff, while malicious nodes take sophisticated risks by evaluating their risk of being identified to decide when to decline. The cluster based routing protocol (CBRP) efficiently minimizes the flooding traffic during route discovery. It is suitable for a small network. In large networks, it provides more overlapping cluster structures which increase the routing overhead so, they proposed ad hoc on demand distance vector (AODV) provides reliable data transmission in MANETs. In AODV, there was a requested source and destination sequence number, which is the essential reason for the routing loop problem and for privacy. This approach minimizes the utility of malicious nodes and it motivates better cooperation between nodes by using the reputation system. Regular nodes monitor continuously to evaluate their neighbors using belief updating systems of the Bayes rule. Even though the regular nodes are follow the PBE strategy to reduce the malicious node utilities for improving throughput in the entire networks. The performance analysis concludes that the PBE strategy was the best strategy for regular nodes to reduce malicious nodes utility. In this analysis, throughput and routing latency are about 91 % respectively, than other protocols that improve the networks performance.

Shen et al. [28] have proposed a QoS-Oriented Distributed routing protocol (QOD) to enhance the QoS support capability of hybrid networks. Taking advantage of fewer transmission hops and any cast transmission features of the hybrid networks, QOD transforms the packet routing problem to a resource scheduling problem. QOD incorporates five algorithms: QoS-guaranteed neighbor selection algorithm to meet the transmission delay requirement, Distributed packet scheduling algorithm to further reduce transmission delay, A mobility-based segment resizing algorithm that adaptively adjusts segment size according to node mobility in order to reduce transmission time, A traffic redundant elimination algorithm to increase the transmission throughput. A data redundancy elimination based transmission algorithm to eliminate the redundant data to further improve the transmission QoS. A number of queuing scheduling algorithms have proposed for Differentiated Service (DiffServ) to further minimize packet droppings and bandwidth consumption. Analytical results based on the random way-point model and the real human mobility model show that QOD can provide high QoS performance in terms of overhead, transmission delay, mobility-resilience and scalability. The traffic redundant elimination based transmission algorithm can further increase the transmission throughput. In the future they placed to evaluate the performance of QOD based on the real test bed.

Liu et al. [29] have proposed a new routing protocol is Authenticated Anonymous Secure Routing (AASR), to satisfy the requirement and defend the attacks. More specifically, the route request packets are authenticated by a group signature to defend the potential active attacks without unveiling the node identities. The key encrypted onion routing with a route secret verification message, was designed to prevent intermediate nodes from inferring a real destination and also check whether AASR can achieve the anonymity goals by three anonymities namely identity anonymity, route anonymity, and location anonymity. To develop the anonymous protocols, a direct method is to anonymize the commonly used on-demand ad hoc routing protocols, such as AODV and ANODR. These results were used to compare the performance of AASR to that of ANODR, in a representative on-demand anonymous routing protocol. The results show that, it provides more throughput than ANODR under the packet-dropping attacks, although AASR experiences more cryptographic operation delay. Compared to ANODR, AASR provides higher throughput and lower packets loss ratio in different mobile scenarios in the presence of adversary attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio. In future, they will improve AASR to reduce the packet delay. A possible method was to combine it with a trust based routing. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks.

Qin et al. [30] have proposed a novel statistical traffic pattern discovery system (STARS). STARS aims to derive the source and destination probability distribution, i.e., the probability for each node to be a message source and destination, and the end-to-end link probability distribution, which is the probability for each pair of nodes to bean end-to-end communication pair. To achieve its goals, STARS includes two major steps one is to Construct point-to-point traffic matrices using the time-slicing technique, and then derive the end-to-end traffic matrix with a set of traffic filtering rules, and next one is Apply a heuristic approach to identify the actual source and destination nodes, and then correlate the source nodes with their corresponding destinations, which use the probability distributions produced by STARS are good indicators of the actual traffic patterns, i.e., actual sources, destinations, and end-to-end links and which reveals most of the actual end-to end links by slightly sacrificing thefalse-positive rate. Specifically, in most cases, more than 80 percent of the actual end-to-end links are revealed (i.e., the false-negative rate was less than 0.2), while the false-positive rate was not more than 0.16.

Li et al. [31] analyze the impact of network load on MAODV protocol, and proposed an optimized protocol

MAODV-BB (Multicast Ad hoc On-demand Vector with Backup Branches), which improves robustness of the MAODV protocol by combining advantages of the tree structure and the mesh structure. The extension of MAODV protocol was to construct a multicast tree with backup branches from two aspects. One is the process of backup branches selection and addition, the other is the mechanism of multicast tree maintenance. It not only can update shorter tree branches but also construct a multicast tree with backup branches. As a tree based multicast routing protocol, M-BB shows an excellent performance in light weight ad hoc networks. Mathematical analysis and this result both demonstrate that the MAODV-BB protocol improves the network performance over conventional MAODV in heavy load ad hoc networks. MAODV-BB's packet delivery was always maintained at a high level even when the network load is heavy also obvious to see that the delay of MAODV-BBis always lower than MAODV's. In MAODV-BB, the existence of backup branches reduces the frequency of tree reconstruction and ensures high packet delivery ratio in heavy load ad hoc networks.

3 Mesh based multicast routing in mobile adhoc network

The group-oriented services are one of the primary applications by mobile ad hoc networks (MANETs) in recent years. To support such services, multicast routing is used. Thus, there is a need to design stable, reliable and secured multicast routing protocols for MANETs to ensure better packet delivery ratio, lower delays, reduce overheads and security mechanism handles misbehaviors and avoid various attacks. To overcome the above problems occurred in MANET, A mesh based multipath routing scheme will proposed in this work. The process flow diagram for proposed routing scheme is illustrated in Fig. 1.

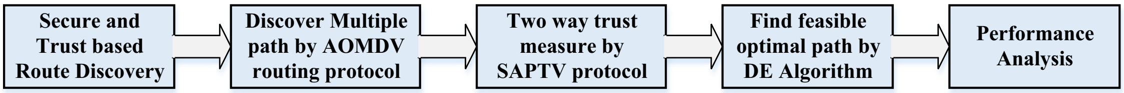
Secure and Trust based Route Discovery
Discover Multiple path by AOMDV routing protocol
Two way trust measure by SAPTV protocol
Find feasible optimal path by DE Algorithm
Performance Analysis

Fig. 1 Proposed flow diagram

3.1 System model assumptions

We make some assumptions before designing the secure adjacent position trust verification framework: (1) In order to ensure the practicality of trust model, we follow the tenet that the 'trust' should be defined and quantified locally. In other words, the trust value is quantified only using the local information for scalability; (2) The communications between two physical neighbours (one-hop) are considered more reliable than those of multi-hop communications; (3) For the purpose of identifying misbehaving nodes, each monitoring node should be equipped with some local detection mechanism (4) The wireless link is symmetrical, while the 'trust'is not necessarily symmetric between two physical neighbourhood entities; (5) The cooperative action in the network interaction is encouraged, which is naturally required in such networks.

Basing on the above assumptions, a mobile ad hoc network with n nodes can be abstracted. Due to the mobile nodes join, leave, or fail over time, the number of n may be dynamically changing. In such networks, trust is a relationship between any two physical neighbour entities, which also can be described as an edge of a directed graph abstracted from the graph theory. Under permitting conditions, each node in the trust system is initially authenticated by an authentication method. In our trust model, every node maintains a trust value for each of its neighbours. This value is a measure of the credible degree of low and high, defined in a continuous range between 0 and 1 (i.e., $0 \leq TV_{ij} \leq 1$). Let $v_i$and v_j denote the monitoring node and the monitored node, respectively. Figure 2 shows the Mesh based multicast routing model for Mobile Ad-hoc Networks (MANETs).

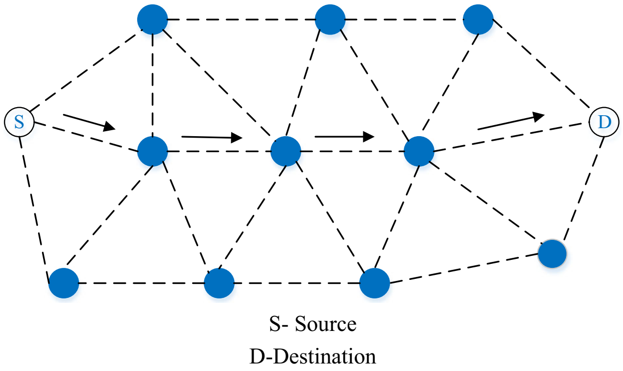

Fig. 2 Mesh based multicast routing

3.2 Secure-trust enhanced ad-hoc on-demand multipath routing protocol (AOMDV–SAPTV)

Our proposed multicast routing scheme can be incorporated into any routing protocol. As an application, a novel trust-enhanced on-demand multi-path routing protocol is proposed (abbreviated as AOMDV–SAPTV), using the standard AOMDV as the base routing protocol. Any mobile node in this trust system has the ability to quantify the trust or reliability for each neighbor and select the trustworthy path to transmit data stream.

3.2.1 Routing table

In this paper, the path trust is determined according to the reliability of each node on this path. The logic is that as soon as any node is untrustworthy, the entire path is untrustworthy. Due to the asymmetry of ‘trust’, this vector can be classified into two types, the secure path trust and the reverse path trust. The former is along the direction of data flow, and the latter is the reverse direction. Precisely speaking, the former represents the subjective judgment of the source, which is used to make a decision whether or not to transmit the data stream by this path. And the later represents the subjective judgment of the destination, whether or not to receive the data stream from this path.

$$SecurePathTrust = \left\{ \begin{array}{r} SecureForwordPathTrust = \min\{TV_{mk}\} \\ s \le m \le d-1 \\ k \le m+1 \\ SecureReversePathTrust = \min\{TV_{km}\} \\ s \le m \le d-1 \\ k \le m+1 \end{array} \right\} \quad (1)$$

where v_s is the sender, v_d is the receiver, v_m and v_k are any two adjacent nodes on the candidate routing path, and $v_m \rightarrow v_k$ denotes that v_k is the next hop of v_m. The routing table entries of proposed routing protocol AOMDV-SAPTV can be seen in Table 1.

According to the above description, two new fields [i.e., *Secure Forward Path Trust* (*SFPT*) and *Secure Reverse Path Trust* (*SRPT*)] are added into the original routing entries of AOMDV–SAPTV, shown in Table 2. *Hop Count*, *Secure Forward Path Trust* and *Secure Reverse Path Trust*, the three metrics compose a three-dimensional evaluation vector for routing decision, which provides a flexible and feasible approach to establish multiple two-way trusted paths.

3.2.2 Secure route discovery

Primarily, the source node begins a network-wide flood by broadcasting a route request packet and waits for route reply packets. Two new fields are added into *RREQ* packet, i.e., Secure Reverse Path Trust (IPT) and Needed Trust (NT). The value of field SRPT is determined based on the minimum of the continued product of trust that the *RREQ* packet has passed on this path, which is initialized to 1 and varies with the packet transmission. We introduce *NT* to represent the path trust requirement, which remaining unchanged during this control packet flooding.

Table 1 Routing entries of AOMDV–SATPV

Destination
Sequence Number
Broadcast Hop Count
Expiration Timeout
Route List $\{(NextHop_1, LastHop_1, HopCount_1,$ $SecureForwardPathTrust_1,$ $Secure\mathrm{Re}versePathTrust_1)$ $(NextHop_2, LastHop_2, HopCount_2,$ $SecureForwardPathTrust_2,$ $Secure\mathrm{Re}versePathTrust_2)$ …… $(NextHop_k, LastHop_k, HopCount_k,$ $SecureForwardPathTrust_k,$ $Secure\mathrm{Re}versePathTrust_k)\}$

RREQ forwarding procedure: After an intermediate node v_j receives an *RREQ* packet from a neighbor nodev_k,

Step 1 If node $v_j$has no route to this neighbor node v_k, it will create a route entry with the filed *Secure Reverse Path Trust* ($SPRT_{kj}$) = RV_{jk}in its local routing table.

Table 2 SPTA packet of AOMDV–SAPTV

<table>
<tr><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type</td><td>N</td><td>P</td><td colspan="14">Reserved</td><td colspan="8">Dest Count</td></tr>
<tr><td colspan="16">Unreachable destination IP Address(1)</td><td colspan="16">Path Id(1)</td></tr>
<tr><td colspan="32">Unreachable Destination Sequence Number(1)</td></tr>
<tr><td colspan="16">Unreachable destination IP Address(2)</td><td colspan="16">Path Id(2)</td></tr>
<tr><td colspan="32">Additional Unreachable destination sequence number(2)</td></tr>
</table>

Step 2 Then it will check whether a similar *RREQ* has been received or not. If so, assume both of the two packets fulfill the trust requirement, while the later copy has no less *Hop Counter* or superior sequence number, then the *RREQ* will be rejected and the process ends; otherwise, go to the next step. On the other hand, if the packets unsuccessful to meet the trust requirement, they will not be forwarded and deleted instantly. Any in-between node may receive multiple *RREQ* copies from other in-between nodes, then go to step 2.

Step 3 If node v_k is not the source, node v_j makes a reverse route to the source using the former hop (node v_k) of the *RREQ* as its next hop. The value of filed *SRPT* is set to min [$SPRT_{sk}$, TV_{jk}] when TV_{jk} is well-known, else the value is min [$SPRT_{sk}$, *Trust_Value*].

Step 4 If node v_j has a valid route to the destination in its routing table, and the routes *Sequence Number* is greater than the *Dest Sequence No* in the *RREQ*, node v_j will generate an *RREP* to node v_k. Otherwise, node v_j modifies the *SRPT* of the *RREQ* using min [$SPRT_{jk}$, TV_{jk}] when TV_{jk} is known, when TV_{jk} is unknown. Then node v_j increases the value of field *Hop Count* by one and propagates this modified *RREQ* packet to all neighbors.

Three new fields are also added into the *RREP* packet. The field *Secure Forward Path Trust (SFPT)* represents the minimum of the continued product of trust that the *RREP* has passed in route reply, which is initialized to 1. The new added field *Needed Trust* (*NT*) has the same meaning as that in the *RREQ*. And the field *Secure Reverse Path Trust* (*SRPT*) is set to min [*SRPT* (obtained in *RREQ*), *SRPT* ($path_{jd}$)]. If an intermediate node has a fresh route to the destination and the received *RREQ* packet has not been processed previously, this node will send a route reply (*RREP*) packet via reversing back the path of *RREQ*. If the destination receives multiple copies of *RREQ*, it will reply the first *k*-paths at most. The parameter *k* is used to control the number of *RREPs* and prevent an *RREP* storm. If an intermediate node receives an *RREP*, it will send the *RREP* via unicast unless the *Secure Forward Path Trust* of the route which the *RREP* has passed is less than the *Needed Trust*. When the *RREP* travels back to the source via traversing the path of the *RREQ*, each node on this path finally can set up a trusted forwarding route.

3.2.3 Secure path trust alert system

In this paper, we propose a novel data-driven route maintenance mechanism, termed as Secure Path Trust Alert. We convert the route error packet into the secure path trust alert packet by adding a new field flag *P*in the reserved field after field *N*, shown in Table 3. The value of Flag *P* set to 1 indicates that the packet is a secure path trust alert packet. When the path trust is lower than the trust requirement value, a path trust alert event will be triggered. The *path id* field could distinguish the different paths via using the *last hop* field in its own routing table entries.

When an intermediate node receives a data packet, it will select its next hop based on the routing entry. And at the same time, it will also confirm whether its potential next hop's trust is larger than the trust value or not. If not, which specifies that the next hop is not a trustworthy node

Table 3 Simulation parameters

Parameters	Details
Simulation tool	Matlab
Node placement	Random
No. of nodes	20, 40, 60, 80, 100
No. of sink (destination)	One
No. of sources	100 (Node 1–100)
Area of simulation	2500 m × 1000 m
Packets generated by each source	250
Total packets generated in N/W	100 × 250 = 2500
Size of each packet	1000 bytes
Initial energy	100 J
Transmission range	250 m
Radio model	Two way ground
Max speed	28 m/s
Traffic type	FTP
MAC	Mac/802_11
Bandwidth	11 mb
Simulation time (in s)	1000 s
Antenna type	Omni directional
Link layer type	LL
Interface queue type	Queue/drop tail
Channel type	Channel/wireless channel
Network interface type	Phy/wirelesss phy

(i.e., suspect or malicious node) and a secure path trust alert event will be activated. In this case, a *SPTA* packet will be sent to its *previous hop* with the help of precursor list in routing table via unicast.

The definitive goal of the system is in response to the sudden or hidden malicious nodes in the routing path, in order to maintain the efficiency of routing. Compared with other trust route maintenance systems this new proposed secure path trust alert system could decrease the routing overhead and route discovery frequency. The main reasons are: (1) This new system is more worthy to the 'trust' criterion, destination, path id rather than only *destination*; (2) the earlier hop of each path in the precursor list is used to govern the propagation range of the route error message.

3.2.4 Loop freedom of AOMDV–SAPTV

On-demand protocols in MANETs may encounter routing loops problem due to that they discover routes with the help of broadcasting mechanism. Sequence number mechanism effectively guarantees loop freedom. That is, for the purpose of avoiding the possibility of any cycle, each node maintains an increasing serial number. Destination sequence number are tagged on all routing packets, so as to provide a mechanism to calculate two relatively fresh routing packets generated two different nodes of the same destination.

An intermediate node creates a reverse path to the source only when receiving a fresh control packet *RREQ*, and a forwarding path to the destination with the *RREP*. At some time, an intermediate node v_j receives a control packet to a destination d ($v_j \neq d$) from a neighbour v_k. The variables *SequenceNumber* k_d, *HopCounter* k_d and *SecureReversePathTrust* k_d represent the *Dest Sequence No*, *Hop Counter* and *Secure Reverse Path Trust* of the control packet respectively. Let $SequenceNumber_{jd}$, $RouteList_{jd}$, $MaxTrust_{jd}$ and $MinHops_{jd}$ be *Sequence Number*, *Route List*, maximum *Secure Path Trust* and minimum *Hop Count* of multiple paths to destination d in the routing table of node v_j respectively. Combined with *RREQ*, the update rule for route entries in routing table is shown as follows.

Loop freedom of AOMDV-SAPTV

```
if ( $SeqNumber_{jd} < SeqNumber_{kd}$ ) then //a new RREQ packet
    $SeqNumber_{jd} = SeqNumber_{kd}$ ;
    $RouteList_{jd}$ =NULL;
    if( $TV_{jk}$ is unknown) then New Secure Reverse Path Trust=min [ $Secure\mathrm{Re}versePathTrust_{kd}$ , Trust_Value];
    else if $TV_{jk}$ >Trust_Value, New Secure Reverse Path Trust=min[ $Secure\mathrm{Re}versePathTrust_{kd}$ , $TV_{jk}$ ];
    insert (k, $HopCounter_{k}$ +1, New Secure Reverse Path Trust) into $RouteList_{jd}$ ;
    node $v_{j}$ rebroadcasts the RREQ;
    else if $TV_{jk}$ <Trust_Value;
    node $v_{j}$ discards this packet;
    end if
   else if ( $SeqNumber_{jd} = SeqNumber_{kd}$ then
    if(min[ $Secure\mathrm{Re}versePathTrust_{kd}$ , $TV_{jk}$ ]>Secure Path Trust_Value and ( $HopCounter_{kd}$ <MinHopsjd-1) then
    if( $TV_{jk}$ is unknown) then New Secure Reverse Path Trust=min( $Secure\mathrm{Re}versePathTrust_{kd}$ , Trust_Value);
    else New Secure Reverse Path Trust=min[ $Secure\mathrm{Re}versePathTrust_{kd}$ , $TV_{jk}$ ];
    endif
    insert (k, $HopCounter_{K}$ +1, New Secure Reverse Path Trust) into $RouteList_{jd}$ ;
    node $v_{j}$ rebroadcasts the RREQ;
    else node $v_{j}$ discards this packet;
    endif
endif
```

As mentioned above, line 1, 4, 8, 11, 12 and 18 of the rule ensures loop freedom. The proposed protocol is only allowed to accept an alternate route with smaller hop count in accordance with meeting the trust requirement.

3.3 Security analysis of AOMDV–SAPTV

Since AOMDV–SAPTV can hide network topology, malicious nodes cannot launch attacks from central positions of the network. Thus, the potential damages incurred by malicious nodes are greatly reduced or even eliminated. Next, we analyse the robustness of AOMDV–SAPTV in resisting the following attacks when the attacks are launched from random positions.

3.3.1 Black hole attack

A black hole attacker disrupts route discovery by forging a route to the destination. A typical attack is launched as follows: When Source S broadcasts a route request to search a route to destination D, attacker ‘A’ replies and advertises a route R_{AD} from itself to destination D. If source S sends packets to destination D via route R_{AD}, the attacker A can intercept and discard the packets. Since AOMDV–SAPTV does not allow intermediate nodes to send route reply messages, it can resist the black hole attack.

3.3.2 Wormhole attack

A typical wormhole attack is launched as follows. Two collaborating attackers first select two central positions in the network to reside such that they are located on many potential routes. Then they build a private tunnel between them and advertise a fake hop count which is smaller than the real hop count between them. The action disrupts the route discovery mechanisms which only use hop count as routing metric since the private channel between the two attackers will always be selected as part of routes considering the smaller hop account. AOMDV–SAPTV can resist wormhole attack because (1) it is topology-hiding and it is impossible for attackers to choose central positions to launch the attack and (2) it uses round-trip time as a routing metric in Route Probe Phase, which makes it robust against hop count modification.

3.3.3 Rushing attack

Rushing attack is one of the denial of service attacks. While a normal node waits for a random delay before sending a packet to avoid collision in wireless communication, a rushing attacker always forwards packets immediately. Because of the rush, the round trip time recorded by a route request is always smaller than the true value if an attacker is on the route, and therefore the route is likely to be selected as the shortest route. AOMDV–SAPTV uses hop count as a routing metric in Route Reply Phase, and thus is resistant to the rushing attack.

3.3.4 Sybil attack

A sybil attacker disrupts route discovery by impersonating multiple legal nodes. To launch this attack, the attacker first obtains the identity of a set of legal nodes and then impersonates some or all of them to participate in multiple route discoveries. AOMDV–SAPTV does not include identity nor topology information in the routing messages, and thus it is impossible for malicious nodes to obtain the identity information of other nodes. Therefore, AOMDV–SAPTV is resistant to sybil attack.

3.4 Enhanced SAPTV with adjacent secure authentication to avoid attacks

We enhance SAPTV by integrating an neighbour authentication mechanism with it. The improved SAPTV can resist more attacks. In the following, we first present the enhanced SAPTV and then analyse its robustness when facing attacks other than aforementioned ones.

Before joining MANET, every node obtains a certificate from a trusted certificate server T. From this certificate, every node has a pair of public key K'_S and private key S'_S, and it keeps its authentication information IMSG:

$$IMSG = \left[t, ID, S'_S(t, ID), K'_S\right],$$

where ‘t’ is the lifetime of the authentication information. The information is used to authenticate the identity of the sender of a route message and verify the message’s integrity. A node always inserts its IMSG into the message it initiates.

Before we present the Route Request Phase with neighbour authentication, we introduce the following notations: S and D represent the source node and the destination node, respectively. A and B represents two intermediate nodes, and N represents a neighbour of the destination. Indicates that the message is sent via broadcasting.

The *RREQ* packet has the following characteristics:

1. The RREQ is anonymous
2. It is transmitted utilizing new, auto generated MAC address,
3. It consists of a public key K'_S taken from M'_S master key of anonymous single-time use keys that don’t permit neighbors to map the key onto a particular node.

We stress that retaining the identity of the verifier is concealed. It is most essential in order to make our AOMDV–SAPTV robust against attacks.

The Route Request Phase has multiple steps:

$$\begin{aligned}
&\text{Step 1: } \underrightarrow{S\ *\ A}\ : RREQ = [[S, Seq, D, hopCt]S'_{s}, IMSG_{S}]\\
&\text{Step2: } \underrightarrow{A\ *\ B}\ : Secure\,\mathrm{Re}\,versePathTrust\\
&\text{Step3: } \underrightarrow{B\ *\ D}\ : RREQ = [[S, Seq, D, hopCt]S'_{s_B}, IMSG_{B}]
\end{aligned}\tag{2}$$

The Route Reply Phase also has multiple steps:

$$\begin{aligned}
&\text{Step 1: } \underrightarrow{D\ *\ N}\ : RREP = [[S, D, nextNode, exNodeSet]S'_{s_D}, IMSG_{D}]\\
&\text{Step2: } \underrightarrow{N\ *\ B}\ : RREP = [[S, D, nextNode, exNodeSet]S'_{s_N}, IMSG_{N}]\\
&\text{Step3: } \underrightarrow{B\ *\ A}\ : RREP = [[S, D, nextNode, exNodeSet]S'_{s_B}, IMSG_{B}]\\
&\text{Step4: } \underrightarrow{S\ *\ A}\ : RREP = [[S, D, nextNode, exNodeSet]S'_{s_S}, IMSG_{S}]
\end{aligned}\tag{3}$$

Neighbour Authentication message interchange protocol-Algorithm

```
Node $S$ do
    $S \rightarrow * : \langle \mathrm{RREQ} = [[\mathrm{S}, \mathrm{Seq}, \mathrm{D}, \mathrm{hopC}_{\mathrm{t}}]S'_{s}, IMSG_{s}]\rangle$
    S: store $t_{s}$
    When receive RREP from $X \subset N_{S}$ do
        S:store $t_{XS}, \langle RREQ = [[S, D, nextNode, exNodeSet\ ]S'_{SD}, IMSG_{D}]\rangle$
    after $T_{\max} + \Delta + T_{random}$ do
        Calculate $T_{\min}$
End
```

With neighbour authentication, before transmitting packets, the source node first verifies the availability of routes and finds the shortest secure route. Then it determines the transmission policy according to the mechanism in based on the number of available routes. When the number of the available routes is less than or equal to three, the source node uses single route policy to forward packet; otherwise, multiple-route policy is applied. The source node restarts the route discovery if there is no available route. The enhanced AOMDV–SAPTV can resist other attacks. For example, modification attack can be detected by authenticating the integrity of route messages. Impersonation attack can be prevented because every node is required to authenticate its neighbours. Fabrication attack can be defeated by appending a signature to route messages.

3.5 Find better link quality optimal path using DE algorithm for data transmission

An optimization technique called DEA is used to find better link quality path to transfer data into our proposed network scheme. DEA can be applied to optimization problems that are partially in dynamic topology changing environment. DEA is applied to find the best nodes involved in a path DEA is meta-heuristic that searches large spaces of candidate solutions. A route with a better link quality is selected for forwarding data from source to destination. If a better link quality is not found, DEA function is performed again until global best solution has been found. DEA reduces the traffic and routing overhead of the optimization process and finds the node with best link quality in an ad hoc network.

3.5.1 DE Algorithm for optimal route selection

The main steps of Dolphin Echolocation (DE) for discrete optimization are as follows:

Initialize nodes (number of echolocations) in a MANET.

In DE (Dolphin Echolocation) algorithm, each location for a dolphin has a search space dimension and a position as follows:

$$d_i(k+1) = d_i(k) + \beta_{1i}(P_i - x_i(k)) + \beta_{2i}(G - x_i(k)) \quad (4)$$

$$x_i(k+1) = x_i(k) + d_i(k+1) \quad (5)$$

where i is the search space index, k is the discrete time index, d_i is the search space dimension of i_{th} location for a dolphin, x_i is position of i_{th} location for a dolphin, P_i is the best position found by km_{winv} location for a dolphin (personal best), G is the best position found by dolphin (global best), β_{1i} and β_{2i} are random numbers in the interval [0, 1] applied to i_{th} location for a dolphin.

The convergence factor should change during the optimization process, should be assigned. Here, the change of CF (Convergence Factor) is considered to be according to the following formula:

$$PP(I_i) = PP + (1 - PP_1)\frac{I_i^P - 1}{(I_N)^P - 1} \quad (6)$$

PP is the predefined probability, PP_1 the convergence factor of the first iteration in which the solutions are selected randomly, I_i the number of the current loop, and Power is the degree of the convergence curve.

In our simulations, the following equation is used for search space dimension

$$d_i(k+1) = \mu(k)d_i(k) + \rho_1[\beta_{1i}(P_i - x_i(k))] + \rho_2[\beta_{2i}(G - x_i(k))] \quad (7)$$

In which μ_k is the inertia function ρ_1 and ρ_2 are the constant factors of search speed. In this paper, linear decreasing strategy has been used in which an initially large inertia weight is linearly decreased to a small value as follows:

$$\mu_k = [\mu(0) - \mu(N_I)]\frac{(N_I - k)}{N_I} + \mu(N_I) \quad (8)$$

where N_I is the maximum number of iterations for which the algorithm is executed, $\mu(0)$ is the initial inertia weight, $\mu(N_I)$ is the final inertia weight. Algorithm 3 describes the steps of the DEA algorithm for optimal weight vector selection to train SVM.

```
Algorithm 3: DEA for optimal weight vector selection

Step 1: Initialize dolphin and randomize the position and search space of each location
$(x_i, d_i; i = 1,........., M)$
Step 2: Calculate predefined probability using equation (6)
Step 3: Compute the fitness function of each location
$(y(i) = fitness(x_i))$.
Step 4: Calculate the accumulative fitness according to dolphin rules
        Alternatives name it as A
for k = -Re to Re
$AF_{(A+k)j} = \frac{1}{\mathrm{Re}} * (\mathrm{Re} - |\, k\, |) fitness(x_i) + AF_{(A+k)j}$
Step 5: Initialize each $P_i$ and $G$ as $P_{i0} = y_i$ and $G = \min(P_{i0}); i = 1,......, M$ .
Step 6:Update the search space of location for a dolphin using dynamic inertia weight (Eqs. (8)
and (19)) and control it by search space clamping as follows:
$d_i(k+1) = \begin{cases} d_i(k+1) & if\ d_i(k+1) < D_{\max} \\ D_{\max} & if\ d_i(k+1) \geq D_{\max} \end{cases}$
        Update the position of location for a dolphin (Eq. (7)).
Step 7: Update $P_i$ and $G$ based on the new value of fitness function as:
$y_{i,new} = fitness(x_{i,new}), P_i = y_{i,new}\ and\ G = \min(P_i)$.
Step 8:If the stop conditions are not satisfied, go to Step 4. Otherwise, stop and return G as the
best solution.
```

DEA is initialized with a group of secure paths and then searches for an optimal route solution by updating generations. Each echolocation is updated by two best values in the iterations. The first one is the best solution that has been achieved previously. The second best value is tracked by the dolphin rules obtained currently by any paths in the population. The bound of the inertial range option is use for providing a satisfactory solution that eventually is discovered. This best value is a global best. The DE algorithm significantly reduces the traffic overhead and computation complexity. The DEA reduced the route failure between nodes that minimize the routing overhead. To decrease the effect of random error, every experiment repeats 50 times and the average of experimental results is used as the performance metrics.

4 Simulation model

To configure proposed secure adjacent position trust verification model, we used the following simulation parameters which we have discussed in Table 3.

4.1 Performance metrics

To maintain the quality of routing the physical parameter analysis will done by analyzing Transmit Energy, Distance, channel load, buffer occupancy, bandwidth and bit error rate (BER).

4.1.1 Transmit energy

We assume that the data transmission between the nodes with power P the corresponding transmit energy is PT_s. Let the variable $E_{s,t}$ be the minimal energy required to transmit one data packet from the source node at (0, 0) to the destination node at (D, 0), and where Z is in decibels over a path with exactly t hops

$$G_t = \frac{E_{st}}{E_{hop}} \tag{9}$$

The normalized minimal transmit energy over a single hop is

$$F_{G1}(g) = P\{E_{s,1} \leq g_{hpo}\} = P\left\{10^{-z/10} \leq g\right\} \tag{10}$$

$$P\left(z \geq -\frac{10}{in10} In\, g\right) = 1 - Q\left(\frac{In\, g}{h\sigma}\right) \tag{11}$$

4.1.2 Distance

The weight function is the parameter $P_{i,j}$ that allows nodes to select the best path. This parameter is defined by:

$$P_{i,j} = \alpha * \frac{D_{i,j}}{T_{r_i}} + \beta * \frac{E_{i,j}}{T_{r_j}} \tag{12}$$

where α and β are the weights satisfied the nodes; $D_{i,j}$ is the distance between node i and node j. T_{r_i} transmission range of node i; T_{r_j} transmission range of node j; $E_{i,j}$ is the maximum energy between node i and node j.

4.1.3 Channel load

This channel load focuses on analyzing the variation of channel load measurements for the nodes. The channel load functionality was implemented by several scenarios were configured for testing. This variation leads us and a usefulness of a single channel load measurement. This channel load measurement can significantly improve the network performance both in network latency and throughput.

4.1.4 Bandwidth

Bandwidth is the rate of data transfer, bit rate or throughput, measured in bits per second. The amount of data that can be carried from one node to another in a given time period is known as bandwidth in MANET. It measures how much data can be sent over a specific connection in a given amount of time. Now days modern networks typically have speeds measured in the millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps). However, this estimate indicates how much bandwidth an application or device in the wireless network can expect when sending or receiving network traffic. This bandwidth variation as on low or high frequency.

Formula for the lower cutoff frequency

$$f_1 = f_0\left(\sqrt{1 + \frac{1}{4Q^2}} - \frac{1}{2Q}\right) \tag{13}$$

Formula for the upper cutoff frequency

$$f_2 = f_0\left(\sqrt{1 + \frac{1}{4Q^2}} - \frac{1}{2Q}\right) \tag{14}$$

Formula for the Q factor

$$Q = \frac{f_0}{f_2 - f_1} \tag{15}$$

Formula for the bandwidth

$$f_2 - f_1 = \frac{f_0}{Q} \tag{16}$$

where f_0 is center frequency f_1 is low cutoff frequency and f_2 is high cut of frequency and Q is the Quality factor

4.1.5 Bit error rate (BER)

Considering a multi hop route between source and destination, the BER at the end of a link between two neighboring nodes, denoted as BER link, depends on the signal-to-noise ratio (SNR) at the receiving node. Finally it is possible to show that the BER at the end of the n_h-th link of the multi-hop route, denoted by BER^{n_k}, can be expressed as

$$BER^{n_k} \cong 1 - \prod_{i-1}^{n_k} [1 - BER_{link}(i)] \tag{17}$$

4.1.6 Through put

It is defined as the total number of packets delivered over the total simulation time. The throughput comparison shows that the three algorithms performance margins are very close under traffic load of 20 up to 100 nodes in MANET scenario and have large margins when number of nodes increases to 100.

Mathematically, it can be defined as:

$$\text{Throughput} = \text{N}/1000$$

where N is the number of bits received successfully by all destinations.

4.2 Results and analysis

The parameters like throughput, transmit energy, channel load, buffer occupancy, transmit distance, bit error rate and packet delivery ratio are improved as previously noted. The parameter analysis of proposed routing scheme can be seen in Table 4.

Figure 3 illustrates a comparison among Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV–SAPTV) in terms of throughput based on random mobility scenario by varying maximum number of connections (number of nodes). The numbers of connections were varied as 20, 40, 60, 80, 100 nodes respectively. At high density like from 100 numbers of connections in Improved AOMDV-AP-overhead improvement (Proposed AOMDV–SAPTV), the throughput increases because of packet lost is too low.

Figure 4 shows that the average end-to-end delay of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV–SAPTV). The average end-to-end delay increases with the increased number of connections. The numbers of connections were

Table 4 Parameter analysis versus number of nodes

Parameters	No of nodes	Throughput (kb/s)	End to end delay (ms)	Transmit energy (J)	Bit error rate (%)	Channel load (%)	Buffer occupancy (%)	Packet delivery ratio (%)
Basic AODV output	20	295	20.3	1586	25.2	24.5	22.8	91.7
	40	614	21.7	3388	20.8	21.9	20.9	92.3
	60	925	22.6	4982	16	19.8	17.1	93.9
	80	1246	23.7	6545	12.8	17.5	15	94.5
	100	1561	24.6	8470	9.1	15.9	12.8	96
Basic AODV with attack	20	286	20.9	1792	27.6	27.5	26.1	90.2
	40	603	22.5	3586	24.3	24.1	23.9	91.1
	60	914	23.2	5187	18	22.8	21	92.8
	80	1235	24.5	6864	14.7	21.1	19.2	93.6
	100	1552	25.5	8779	11.9	19.9	18.1	94.9
AODV with attack prevention	20	300	20.1	1516	23.3	24.5	20.1	93
	40	618	21	3246	17.5	19.2	18.6	94.5
	60	935	21.9	4874	13.9	17.5	15.7	95.2
	80	1254	23	6432	10.7	14.9	13.4	96
	100	1571	23.8	8308	7.1	13.5	11	96.9
AODV with attack prevention but changes in overhead	20	305	19.2	1465	20.5	23.1	18	94.1
	40	624	20	3032	15.4	18.4	16.1	95.3
	60	942	20.9	4710	11.2	16.1	12.9	96.1
	80	1435	22.1	6310	8.9	13.9	11.2	96.9
	100	1705	23	8202	6.1	11.1	9	98.1
Improved AODV with attack prevention but improvement in overhead	20	317	18.3	1210	15.6	20.5	14.9	95
	40	637	19.1	2754	12.3	17.4	11.8	96.2
	60	956	20	4453	8.8	14.2	9.7	97
	80	1564	21.2	6309	6.3	11	6.8	98.2
	100	1787	22	8001	5	8.3	5	99.1

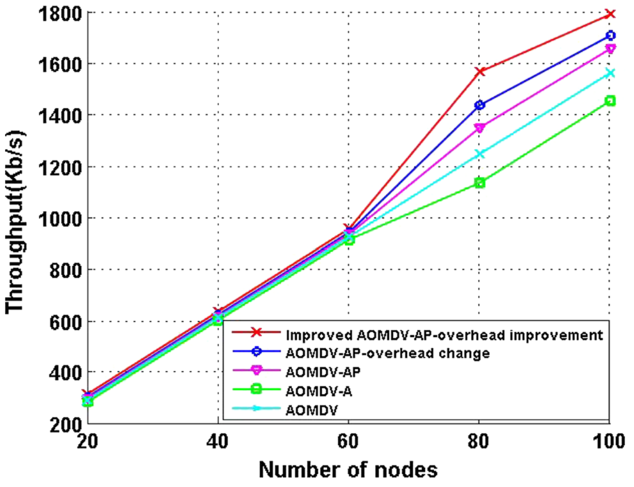

Fig. 3 Measurement of throughput varying maximum number of nodes (Kb/s)

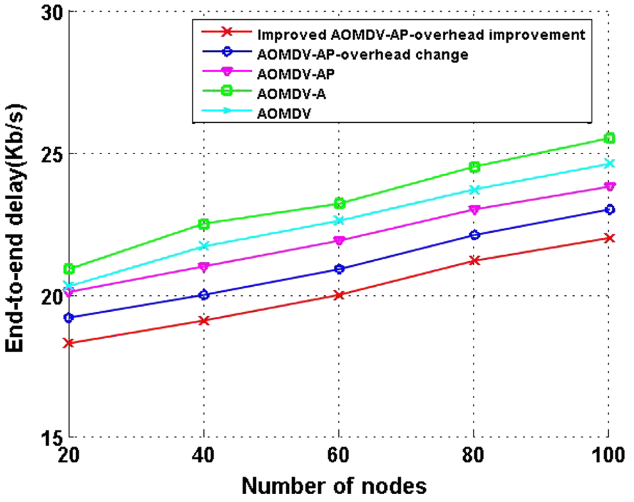

Fig. 4 Measurement of end to end delay varying maximum number of nodes (ms)

varied as 20, 40, 60, 80, 100 nodes. After increasing number of connections more than 40, end-to-end delay increase much higher because of queuing and retransmission delay. In heavy traffics load as the maximum number of connections increase, the number of packets delivery also increase. But based on the above graph comparison end to end delay for our proposed AOMDV–SAPTV is very low.

Figure 5 shows transmission energy of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV–SAPTV) and the maximum number of connections energy consumption respectively. Based on the above graph comparison shows that our proposed protocol AOMDV–SAPTV consumes low energy compared to others. The life time (battery) of the node for AOMDV–SAPTV is higher than other protocol. In the case of a link failure, AOMDV–SAPTV has the ability to make longer battery and node's life time because of the proper utilization in choosing a path.

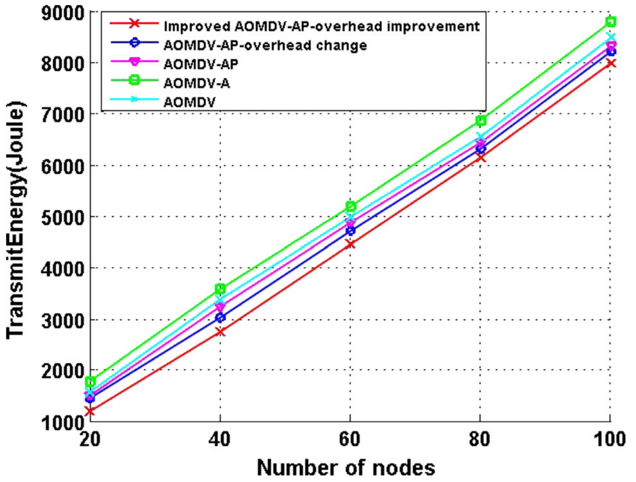

Fig. 5 Measurement of transmission energy varying maximum number of nodes (J)

Figure 6 shows Bit Error Rate of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV–SAPTV). Above graph comparison shows Bit Error rate is too low for our proposed AOMDV–SAPTV protocol because of high low packet loss.

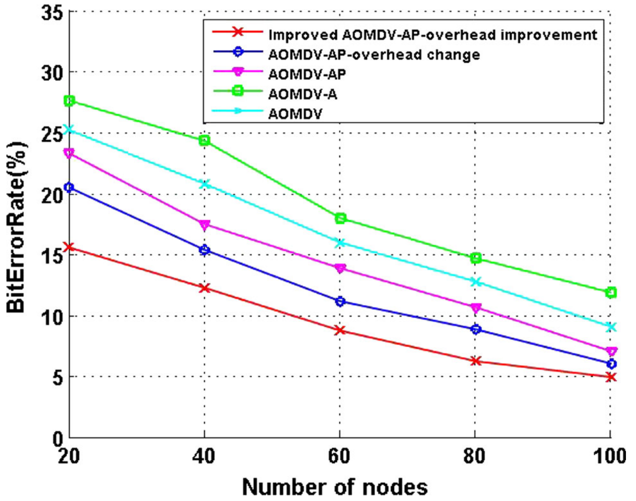

Fig. 6 Measurement of bit error rate varying maximum number of nodes

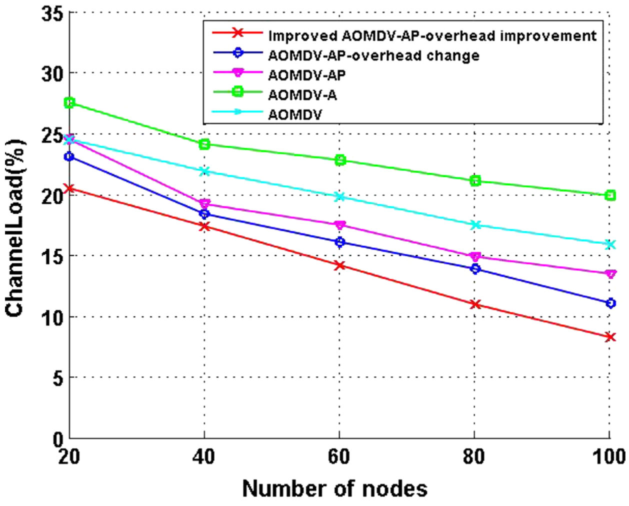

Fig. 7 Measurement of channel load varying maximum number of nodes

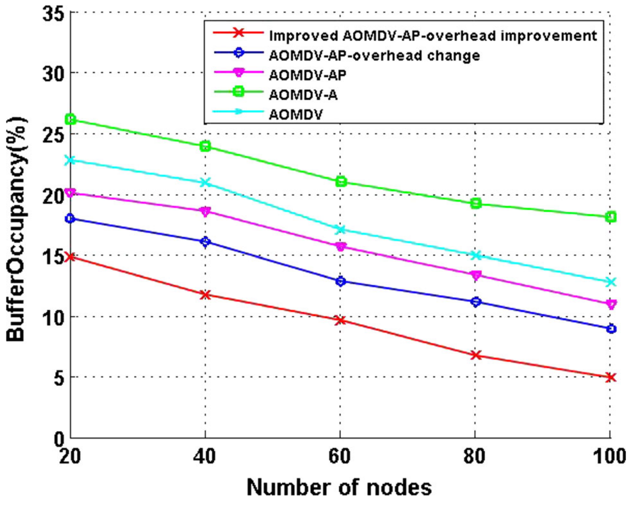

Fig. 8 Measurement of buffer occupancy varying maximum number of nodes

Figure 7 shows channel load percentage of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV–SAPTV). Above graph comparison shows channel load percentage is too low for our proposed AOMDV–SAPTV protocol because of traffic occurrence level is very low.

Figure 8 indicates the effect of buffer occupancy ofBasic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV–SAPTV). Above graph shows the proposed routing protocol AOMDV-SAPV using the multipath but congestion avoiding ability of proposed protocol gives better throughput then the AOMDV. AOMDV–SAPTV uses the buffer space of the neighboring node so packet drop is less as compared to the AOMDV. So it shows that AOMDV–SAPTV is better than AOMDV.

Figure 9 shows packet delivery ratio of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV–SAPTV). Above graph comparison shows PDR rate is too high for our proposed AOMDV–SAPTV protocol because of secure trust based optimal route selection.

Based on the above parametric matrices like throughput, transmit energy, channel load, buffer occupancy, transmit distance, bit error rate and packet delivery ratio are improved compared to other existing routing protocols. It denotes our proposed AOMDV–SAPTV provides better quality of service (QoS) and security against vulnerabilities.

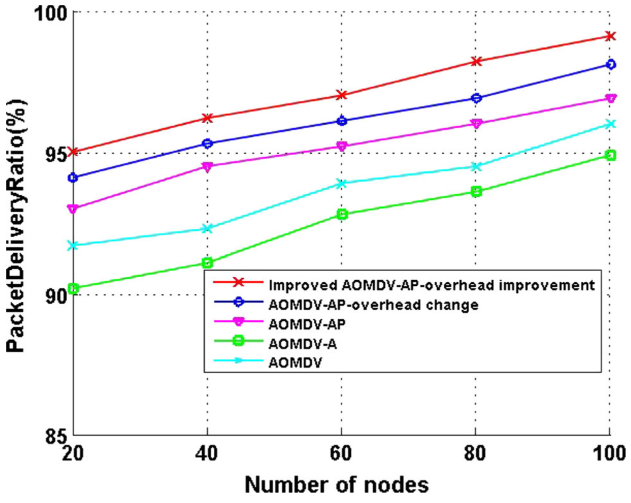

Fig. 9 Measurement of packet delivery ratio varying maximum number of nodes

5 Conclusion

Mobile ad hoc networks have attracted much interest in the research community due to their potential applications. However, the inherent characteristics of such networks make them vulnerable to a wide variety of attacks. The security concerned in these wireless networks remains a serious impediment to widespread adoption. In this paper, we focus on the security of routing protocol in MANETs. Firstly, we abstract a secure adjacent position trust verification model. Then by extending the standard ad hoc on-demand multi-path distance vector protocol (AOMDV), we propose a novel secure adjacent trust-enhanced routing protocol combined with the trust model, named as AOMDV–SAPTV. The persuasive experiments have been conducted to simulate and present the effectiveness of this new protocol. The main purpose of QoS aware routing is to find a feasible path from source to destination which will satisfy two or more end to end QoS constrains. The DE algorithm is used to find the optimal and best path for routing. The proposed scheme is compared to the existing routing protocols. The result shows that our proposed technique enhanced the quality of routing and had find the best path by the optimization algorithm.

References

1. Corson, M. S., Macker, P. J., & Cirincione, G. H. (1999). Internet-based mobile ad hoc networking. *Internet Computing, IEEE, 3*(4), 63–70.
2. Attar, A., Tang, H., Vasilakos, A. V., Yu, F. R., & Leung, V. (2012). A survey of security challenges in cognitive radio networks: Solutions and future research directions. *Proceedings of the IEEE, 12*(100), 3172–3186.
3. Cordasco, J., & Wetzel, S. (2008). Cryptographic versus trust-based methods for MANET routing security. *Electronic Notes in Theoretical Computer Science, 197*(2), 131–140.
4. Azedine, B., El-Khatiba, K., Xua, L., & Korbab, L. (2005). An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks. *Computer Communications, 28*(10), 1193–1203.
5. Li, Wenjia, & Joshi, Anupam. (2008). *Security issues in mobile ad hoc networks—A survey* (pp. 1–23). Baltimore County: Department of Computer Science and Electrical Engineering, University of Maryland.
6. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks, 20*(8), 2481–2501.
7. Yang, Hao, HaiyunLuo, Fan Ye, Songwu, Lu, & Zhang, Lixia. (2004). Security in mobile ad hoc networks: Challenges and solutions. *Wireless Communications, IEEE, 11*(1), 38–47.
8. Wei, L., Zhu, H., Cao, Z., Jia, W., & Vasilakos, A. V. (2010). Seccloud: Bridging secure storage and computation in cloud. In *IEEE 30th International Conference on 2010 distributed computing systems workshops (ICDCSW)* (pp. 52–61).
9. Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *Communications Magazine, IEEE, 40*(10), 70–75.
10. Mohapatra, P., Li, J., & Gui, C. (2003). QoS in mobile ad hoc networks. *IEEE Wireless Communications, 10*(3), 44–53.
11. Wu, C., Zhang, F., & Yang, H. (2010). A novel QoS multipath path routing in MANET. *International Journal of Digital Content Technology and its Applications, 4*(3), 132–136.
12. Jiang, S., Liu, Y., Jiang, Y., & Yin, Q. (2004). Provisioning of adaptability to variable topologies for routing schemes in MANETs. *IEEE Journal on Selected Areas in Communications, 22*(7), 1347–1356.
13. Wan, J., Liu, J., Shao, Z., Vasilakos, A. V., Imran, M., & Zhou, K. (2016). Mobile crowd sensing for traffic prediction in internet of vehicles. *Sensors, 16*(1), 88.
14. Dvir, A., & Vasilakos, A. V. (2011). Backpressure-based routing protocol for DTNs. *ACM SIGCOMM Computer Communication Review, 41*(4), 405–406.
15. Zhang, X. M., Zhang, Y., Yan, F., & Vasilakos, A. V. (2015). Interference-based topology control algorithm for delay-constrained mobile ad hoc networks. *Mobile Computing, IEEE Transactions, 14*(4), 742–754.
16. Vasilakos, A. V., Zhang, Y., & Spyropoulos, T. (Eds.). (2011). *Delay tolerant networks: Protocols and applications*. Boca Raton: CRC Press.
17. Vasilakos, A. V., Li, Z., Simon, G., & You, W. (2015). Information centric network: Research challenges and opportunities. *Journal of Network and Computer Applications, 30*(52), 1.
18. Yao, G., Bi, J., & Vasilakos, A. V. (2015). Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter. Information Forensics and Security. *IEEE Transactions, 10*(3), 471–484.
19. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications, 42*, 120–134.
20. Yang, H., Zhang, Y., Zhou, Y., Fu, X., Liu, H., & Vasilakos, A. V. (2014). Provably secure three-party authenticated key agreement protocol using smart cards. *Computer Networks, 58*, 29–38.
21. Liu, B., Bi, J., & Vasilakos, A. V. (2014). Toward incentivizing anti-spoofing deployment. *Information Forensics and Security, IEEE Transactions, 3*, 436–450.
22. Zhou, J., Cao, Z., Dong, X., Xiong, N., & Vasilakos, A. V. (2015). 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. *Information Sciences, 314*, 255–276.
23. Wei, L., Zhu, H., Cao, Z., Jia, W., & Vasilakos, A. V. (2010). Seccloud: Bridging secure storage and computation in cloud. In *2010 IEEE 30th international conference distributed computing systems workshops (ICDCSW)* (pp. 52–61).
24. Wang, T., Liu, Y., & Vasilakos, A. V. (2015). Survey on channel reciprocity based key establishment techniques for wireless systems. *Wireless Networks, 21*(6), 1835–1846.
25. He, D., Chen, C., Chan, S., Bu, J., & Vasilakos, A. V. (2012). Re Trust: Attack-resistant and lightweight trust management for medical sensor networks. *Information Technology in Biomedicine, IEEE Transactions, 16*(4), 623–632.
26. Zhou, J., Dong, X., Cao, Z., & Vasilakos, A. V. (2015). Secure and privacy preserving protocol for cloud-based vehicular DTNs. *Information Forensics and Security, IEEE Transactions, 10*(6), 1299–1314.
27. Paramasivan, B., Prakash, M. J. V., & Kaliappan, M. (2015). Development of a secure routing protocol using game theory model in mobile ad hoc networks. *IEEE Journal of Communications and Networks, 17*(1), 75–83.
28. Shen, H., & Li, Z. (2014). A QoS-oriented distributed routing protocol for hybrid wireless networks. *IEEE Transactions on Mobile Computing, 13*(3), 693–708.
29. Liu, W., & Yu, M. (2014). AASR: Authenticated anonymous secure routing for MANETs in adversarial environments. *IEEE Transactions on Vehicular Technology, 63*(9), 4585–4593.
30. Qin, Y., Huang, D., & Bing, Li. (2014). STARS: A statistical traffic pattern discovery system for MANETs. *IEEE Transactions on Dependable and Secure Computing, 11*(2), 181–192.

31. Li, X., Liu, T., Liu, Y., & Tang, Y. (2014). Optimized multicast routing algorithm based on tree structure in MANETs. *China Communications, 11*(2), 90–99.

Gautam M. Borkar received his Bachelors degree from National Institute of Technology, Jalandhar, Punjab, India and completed his masters from Sant Gadge Baba Amravati University, Amravati Presently he is working as Assistant Professor in Rajiv Gandhi Institute of Technology, Mumbai and pursuing Ph.D. from Sant Gadge Baba Amravati University, Amravati His current research interest includes network security, trust management and security in wireless sensor network.

Dr. A. R. Mahajan is working as Head, Department of Information Technology, Government Polytechnic College, Nagpur, India. She has obtained her Ph.D. in Computer Science and Engineering. She has published twenty four papers in international journals and one in national journal. She has presented forty three and five papers in international conferences and national conferences, respectively. She has more than 20 years of teaching and research experience. Her area of specialization is compiler optimization, artificial intelligence, parallel algorithms. She is a member of IEEE, ISTE and CSI.