International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 6611-6630

http://www.ripublication.com

Trust Based Multipath Routing To Mitigate Wormhole Attack

[1]Ramya Dorai and [2] Rajaram. M

[1]Adhiyamaan College of Engineering, Department of Computer Science Engineering, Hosur, 635109, Tamilnadu, India ramyadorai.aom@gmail.com
[2]Vice-chancellor, Anna University, Chennai, Tamilnadu, India

Abstract

Mobile Adhoc Networks (MANETs) are vulnerable to attacks due to its characteristics like open medium, distributed nodes, node autonomy, network participation, lack of centralized authority which enforces network security, distributed co-ordination and cooperation. Worm hole, in cosmological terms, connects two distant points in space through a short route. Similarly also one or more attacking node can disrupt routing by short-circuiting the network and disrupting packet flow in a MANET.This work proposes a novel trust mechanism to mitigate the wormhole attack in MANETs. The proposed protocol is based on Adhoc On-Demand Multi-Path Distance Vector (AOMDV).

Keywords: Mobile Adhoc Network (MANET), Adhoc On-demand Multi-Path Distance Vector (AOMDV), Wormhole attack, Trust and Reputation

1. INTRODUCTION

MANETs are a collection of wireless mobile nodes that dynamically exchange data between themselves without relying on a fixed base station or wired backbone network. MANETs have much use in various, disparate situations including battlefield communications to disposable sensors dropped from high altitudes and dispersed on ground for hazardous material detection. Civilian applications include scenarios like people at a conference in a hotel where their laptops are temporary MANETs to more complicated scenarios like highly mobile vehicles on a highway which form an adhoc network to ensure traffic management [1].

Routes are mainly multi hop in adhoc mobile networks, due to limited radio propagation range and frequent topology changes and unpredictably as each network hosts move randomly. So, routing is an integral part of adhoc communications. To facilitate communication within network, a routing protocol discovers routes between nodes [2]. An adhoc network routing protocol's goal is correct and efficient route establishment between a node pair so that messages are delivered in time. Route construction should be done with minimum bandwidth consumption and overhead. An adhoc routing protocol is a convention or standard controlling, how nodes agree which way to route packets between computing MANET devices.

Routing is to find and maintain routes among nodes in a dynamic topology with maybe uni-directional links, using minimum resources [3]. Routing, transfers a packet from source to destination. In routing, a mobile node searches for path or route to communicate with other network nodes. Protocols are rules through which two or more devices communicate with others. MANETs use routing tables for routing. They have route information to all mobile nodes [4].

MANET routing protocols plays a basic role in ubiquitous devices. Current MANET commercial applications are for military applications or emergency situations. A MANET is a system of autonomous mobile nodes communicating over wireless links without preinstalled infrastructure. MANET routing protocols are classified into three categories

- Proactive or Table Driven Routing Protocols,
- Reactive or On-Demand Routing Protocols,
- Hybrid Routing Protocols.

Multipath routing has lent itself to be of use for connection-oriented networks; call blocking probability is pertinentto connection oriented networks. Multipath routing includes finding multiple routes between source and destination nodes and share paths between source and destination node pairs and compensate adhoc networks dynamic and unpredictable nature.

Multipath routing establishes multiple paths between source-destination pairs and requires more hosts for routing. Though many benefits were explored for wired networks multipath routing, its advantage is not obvious in MANETs as traffic on different paths may interfere with others due to radio transmission broadcast feature [5]. Multipath routing has 3 components: route discovery, route maintenance, and traffic allocation.

To discover multiple paths from source to a destination, basic route discovery mechanism used in DSR and AODV protocols need modification. One reason for using multipath routing is discovering multiple paths that must be node-disjointed or link disjointed [6]. In node-disjointed paths, path nodes should not be common. In link-disjointed paths, path links should not be common. When multiple paths are discovered, multipath routing protocol decides to select path to send data packets. When a path or set of paths are selected, a good multipath routing protocol decides how to use them when sending data packets. Advantages of Multipath Routing:

1. load balancing,
2. fault-tolerance,
3. higher aggregate bandwidth

Security means security mechanism for protocols involved in MANET service to protect basic functions and also means security during bit transfer from a node to another. Adhoc networks security services are not different from other network communication paradigms. The aim is protecting information and resources from attacks/misbehavior. In network security, the requirements of an effective security paradigm are explained:

Availability: ensures availability of desired network services when expected, despite attacks. Systems ensuring availability combat denial of service and energy starvation attacks that are presented later.

Authenticity: ensures that communication from a node to another is genuine. It ensures that malicious nodes cannot masquerade as trusted network nodes.

*Data confidentiality:*adhoc networks core security primitive, ensuring that a given message is not understood by anyone other than desired recipient. Data confidentiality is enabled through cryptography [7].

Integrity: denotes data authenticity when sent from a node to another. It ensures a message from node A to node B is not modified by malicious nodes, C, during transmission. A robust confidentiality mechanism ensures data integrity adding one way hashes to encrypted messages.

Non-repudiation: ensures that message origin is legitimate, i.e. when a node receives a false message from another, non-repudiation allows former to accuse latter of sending false messages and enabling other nodes to learn of it. Digital signature ensures non-repudiation.

Security has 2 approaches [8]:

A. Proactive:-This thwarts security threats through cryptographic techniques.

B. Reactive: First detects threat and reacts. Due to absence of a clear defence, a complete MANET security solution involves both approaches. So a way to check security is **Prevention, Detection** and **Reaction**.

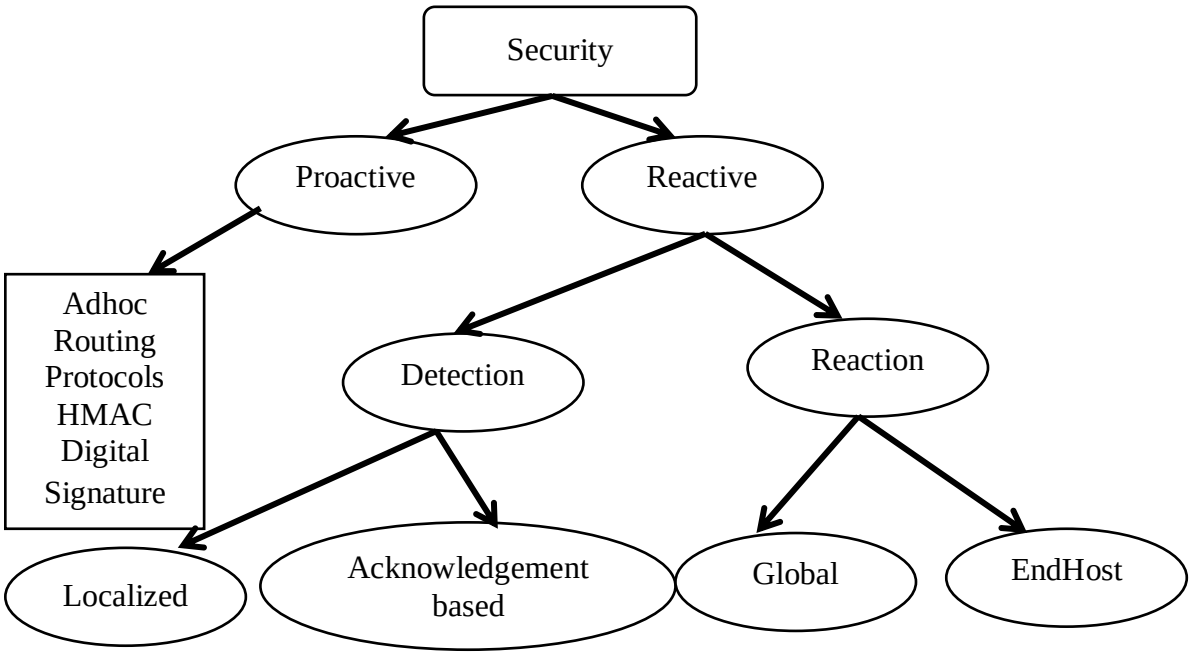

Figure 1 Security approaches in MANET

Communication security in MANET is important to ensure secure information transmission. Absence of a central co-ordination mechanism and shared wireless medium makes MANET vulnerable to digital/cyber-attacks than wired network. There are many attacks affecting MANETs and are classified as [9]:

1. External Attack: these are carried out by nodes not of the network. It motivates congestion and sends false routing information or makes services unavailable.

2. Internal Attack: are from compromised network nodes. In such attacks malicious network nodes gain access and impersonate genuine nodes.It analyzes traffic between other nodes and participates in other network activities.

Attacks against routing messages are in many forms and include all characteristics described earlier. Information/messages can be deviated from normal operation flow using interception, interruption, modification, or fabrication attacks

[10].

An attacker exhausts network resources in flooding attack like bandwidth. They consume a node's resources like computational and battery power or disrupt routing causing severe network performance degradation [11]. In blackhole attacks, a malicious node sends fake routing information, claiming an optimum route causing other good nodes to route data packets through the malicious node. In link spoofing attacks, malicious nodes advertise fake links with non-neighbors to disrupt routing operations.

A definition considers trust as a measure of subjective belief that a person or party uses to assess the probability that another will perform a favorable action before a chance to monitor whether the activity occurred presents itself. When a person is trustworthy; it means that there is a high probability that actions they are expected to perform are done in favorable manner to the trustor. Measurements like integrity, ability and benevolence are properties to measure trust [12]. These have a considered correlation with overall trust measure that changes with time.

A consideration that is important to MANET security is that trust is required in developing relationships during uncertainty [13], which matches MANET problems where the unforeseen is a concern [14].An entity's reputation, on the other hand, is an expectancy of its behavior based on other entities' observations or information about entity's past behavior in a specific context at a time [15].

The trust manager's main functionality is reputation information management involving 4 activities [16]:

1. Reputation information collection,
2. Reputation information formatting,
3. Reputation information maintenance, and
4. Reputation information rating.

MANETs are more vulnerable than wired networks to attacks.Security is a challenge in MANETs. This study proposes a new trust mechanism to mitigate wormhole attack in MANETs. The study is organized as follows: Section 2 discusses related works and section 3 explains methodology. Section 4 discusses experimental results and section 5 concludes the work.

2. RELATED WORK

Performance analysis of AOMDV routing protocol was discussed by Kute et al., [17]. AOMDV is a multipath extension of AODV. Different QoS issues were discussed for MANETs and AOMDV's different QoS issues with varying data packet generation rate were analyzed. From simulation it is concluded that increased packet rate degraded AOMDV performance for CBR traffic while it is consistent for TCP traffic. In future work, AOMDV would be analyzed regarding mean node speed, which was constant.

Trusted routing protocols using trusted frame works and intrusion detection system (secure protocol) for MANETs was designed by Sharma [18]. The model provided trust combination algorithms and trust mapping functions. The new trust model ensures trusted MANET routing protocols called TAODV on AODV routing protocol. Wireless networks security and selfishness issues were implemented either in non-cooperative or cooperative form. Experiment results revealed that cumulative utilities of cooperative nodes increased steadily and selfish nodes were unable to get utilities by behaving selfishly. .

A multi-dimensional trust management framework to ensure improved evaluation of MANET nodes trustworthiness was proposed by Li et al., [19]. The proposed approach's contributions include: (1) multi-dimensional trust management framework where trustworthiness notion is classified into many dimensions so that all dimensions can indicate whether a node is trustworthy regarding one specific behavior that it should conduct like cooperation, behaving well and being honest; and (2) an adaptive trust evolution model where all trustworthiness dimensions are adjusted according to misbehavior features to which the dimension is related like outcome severity, occurrence frequency and context where misbehavior occurs.

An overview of MANET routing protocols was presented by Agrawal et al., [20] who also reviewed current state of the art routing attacks and countermeasures. Advantages and countermeasures drawbacks were outlined. Most proposed solutions work only with one or two specific attacks being vulnerable to unexpected attacks. Future research should focus on improving security schemes effectiveness and also minimize cost to make them suit MANET environments.

A Trust Based Reliable AODV (TBRAODV) protocol which implemented a trust value for all MANET nodes was presented by Subramanian et al., [21]. Trust value was calculated for each node and based trust value nodes participated in routing or were identified to become a misbehaving node. This enhanced AODV routing reliability and resulted in PDR increase, delay decrease and maintenance of

throughput. The new work was implemented and simulated on NS-2. Based on simulation, the new protocol ensured consistent and reliable data transfer compared to general AODV, when there were misbehaving nodes in MANETs.

A threefold method to formalize and evaluate trust, to use trust to establish keys between MANET nodes and use trust as a metric to establish secure distributed control in MANETs was proposed byFerdous et al., [22]. Nodes metrics were defined to establish/manage trust and reviewed adhoc networks routing protocols with trust considerations.

Basic MANET routing protocols like Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR), Temporally-Ordered Routing Algorithm and Adhoc On demand Distance Vector (AODV) were discussed by Jhaveri et al., [23]. Security is a big MANET issue due to their beinginfrastructure-less and autonomous. The aim of the new work was addressing basic MANET security concerns, wormhole attack operation and securing AODV. The new work used Trustworthy techniques to detect wormhole attacks.

Performance of AODV (unipath) and Adhoc On-demand Multi path Distance Vector (AOMDV) routing protocol were evaluated and compared byBalakrishna et al., [24]. AODV and AOMDV performances were evaluated with Advent Net Simulator. Comparison was based on packet delivery ratio, incurred routing overhead, average end-to-end delay and packets dropped. It concluded that AOMDV was better than AODV. AOMDV outperformed AODV because of its ability to search for alternate routes when a link broke. Though AOMDV had more routing overheads when flooding network and packet delays due to alternate route discovery mechanism, it is more efficient in packet delivery for similar reason.

Performance of MANET under wormhole attack was analyzed by Maulik et al., [25]. Multiple QoS parameters were considered in the new work for delay, throughput, packet delivery ratio, node energy, and node density to be manipulated. NS2 network simulator was used, and Reference Point Group Mobility Model (RPGM) studied node density effect and initial energy on throughput. The new work focused on QoS being affected by a wormhole attack and established foundation for future work toward designing a mechanism to identify nodes and links actively involved in wormhole attacks.

A mechanism called AODV-Wormhole Attack Detection Reaction (AODV-WADR) to secure eMANETs against wormhole attacks was proposed by Panaousis et al., [26]. Simulations were done on ns-2 proving that AODV-WADR did not introduce high overhead and reduced packet loss due to malicious wormhole nodes

greatly. AODV-WADR needs no statistical methods, GPS coordinated or specialized hardware, as using such methods or hardware is not practical in eMANETs.

Trust concepts and properties were discussed by Cho et al., [27] who derived unique trust characteristics in MANETs, drawing upon social trust notions. A survey of trust management schemes for MANETs was provided, and discussed accepted classification, potential attacks, performance metrics and trust metrics.

How mobile devices, energy consumption and their density affected MANET performance was analyzed by Murali et al., [28]. AODV and AOMDV are reactive MANET routing protocols handling link break caused by node mobility and energy drain. AODV and AOMDV performance were analyzed in link breaks through ns2 simulator. Results proved that AOMDV performed better in throughput, end to end delay and packet delivery ratio compared to AODV in large networks with high node mobility. Compared to AODV, energy consumption and normalized routing load was high for AOMDV for all scenarios.

A Stability-based Partially Disjoint AOMDV (SPDA) protocol which was a modification of AOMDV protocol was presented by Al Mobaideen et al., [29]. Based on links stability, SPDA found partially disjoint paths,the idea being that accepting partially disjoint paths that were stable than other maximally disjoint ones increased path life. This improved MANET performance regarding delay, routing packets overhead, and network throughput. Results of some experiments using Golomosim simulator package, showed improved performance in the new protocol regarding performance metrics.

Fully distributed reputation-based mechanisms that improved MANET security was the concern of Kumar and Parthipan [30] which implemented a cognitive and optimized method to calculate nodesreputation. Eigen vector and Degree centrality was proposed for individual trust value evaluation. They designed and built a NS2 over DSR prototype, in presence of a Worm Hole Attack in highly mobile and hostile environments.

Criterion for successful wormhole attack on MANET was analyzed by Mahajan et al., [31]. Based on results from Qualnet simulation, likelihood of such attack was evaluated. Wormhole scenarios were classified into successful, unsuccessful, doubtful, interesting, and uninteresting which also defined wormhole strength. It was observed that detection ratio of technique varied with wormhole strength and network topology. Simulation statistics showed that wormholes with higher strength had higher detection ratio compared to those with lower strength.

3. METHODOLOGY

AOMDV protocol based trust and reputation based mitigation schemes for wormhole attack is discussed in this section.

3.1 Adhoc On-demand Multi path Distance Vector Routing (AOMDV)

AOMDV protocol is an extension of AODV protocol to compute multiple loop-free and link disjoint paths [32]. Routing entries for destinations have a list of next-hops with corresponding hop counts. All next hops have same sequence number which helps to track a route.

AOMDV can find node-disjoint or link-disjoint routes. To find node-disjoint routes, a node does not reject duplicate RREQs immediately. Every RREQs arriving through a different source neighbor defines node-disjoint path as nodes cannot broadcast duplicate RREQs. So any 2 RREQs arriving at an intermediate node through different source neighbors cannot have traversed same node. To get multiple link-disjoint routes, destination replies to duplicate RREQs, destination only replies to RREQs arriving through unique neighbors. After first hop, RREPs follow reverse paths, which are node disjoint and so link-disjoint. Each RREP's trajectories may intersect at an intermediate node, but all take different reverse paths to source to ensure link disjointness [33].

Using AOMDV allows intermediate nodes to reply to RREQs, when selecting disjoint paths. But, AOMDV has more message overheads during route discovery due to increased flooding and as it is a multipath routing protocol, destination replies to multiple RREQs, results are in longer overhead.

3.2 Wormhole Attack

Wormhole attack is an efficient and merciless attack, executed within MANETs. Two collaborating attackers establish a so called wormhole link (through private high speed network e.g. Ethernet cable/optical link): connection via a direct low-latency communication link between two separated distant points in MANETs. When this direct bridge (wormhole link) is built, one attacker captures data exchange packets, sends them via wormhole link to second one which replays them.

Wormhole attacks are dangerous against adhoc network routing protocols where nodes hearing a packet transmission directly from a node consider themselves in range of (and so a neighbor of) that node. For example, when used against routing protocol like DSR or AODV, a powerful wormhole attack can be mounted by tunneling ROUTE REQUEST packet directly to destination target REQUEST node.

When destination node's neighbors hear the REQUEST packet, they follow normal routing protocol processing to rebroadcast the REQUEST copy and discard other received ROUTE REQUEST packets from same Route Discovery [34] without processing.

Classification of Wormhole Attack

The wormhole attack is invisible at higher layer and so, two wormhole end points are invisible on the route where detection is more complex. Wormhole is classified into 5 categories as proposed,

1. Wormhole using Encapsulation.
2. Wormhole using out of band channel.
3. Open wormhole attack.
4. Closed wormhole attack.
5. Half open wormhole attack.
6. Wormhole with high power transmission.

3.3 Trust

MANETs offer many unique properties that create differing considerations to determine trust:

- Self-organisation means they are autonomous, with no fixed infrastructure and centralised administrative node.
- End-to-end communication requires packet forwarding for information to reach required destinations, and nodes must communicate with neighbouring nodes with confidence.

A highly dynamic topology requires reliable and scalable security mechanisms which take into account of the constraints such as Bandwidth, Computer power, and Battery power in mobile devices.Current trust management perception for network security was first conceptualized with PolicyMaker [35]; a distributed trust management framework that delved into “trust management problem”, moving trust security from simple third party certificating. This ensured flexibility to support trust relationships and localized control through binding public keys to access control without hard security authentication. The subjective trust value was realized by each party/node in a network, rather than globally. Though localized, the paper did not

boast a decentralized concept, but relied on a localized "trust management engine" queried for policy information [36].

In this work, a collaborative mechanism is used to compute direct trust and indirect trust is computed based on adaptive statistical profiling technique by filtering the route replies. A collaborative detection strategy is resorted to when a node monitors control traffic in and out of neighbors. For a node, say α, to watch a node, say β, α should be a neighbor of both β and previous hop from β, say δ. Then α is called guard node for link from δ to β. For example nodes M, N, and X are guard nodes of A over link from X to A. Information from every packet from X to A is saved in a watch buffer at each guard.

Guards expect A to forward packet to ultimate destination, unless A is the destination. Each entry in watch buffer is time stamped with time threshold, τ, by which A must forward packet. Each packet forwarded by A with X as a previous hop is checked for corresponding information in watch buffer. Check verifies if packet is fabricated or duplicated (no corresponding buffer entry), corrupted (matching payload hash), dropped or delayed (entry is not matched in τ).Guard nodes maintain a trust counter *(Trust(i,j))i,* for a node, *j*, at receiving end of a link that *i* is monitoring over a sliding window of length T_{win}. *Trust (i,j)* is incremented for Trust activity of *j* detected by *i*. Increment to *Trust*depends on malicious activity's nature [37]. When growth in counter value maintained by guard node a for node A *(Trust (a,A))* crosses threshold rate *(Trust th)* over T_{win}, node α revokes A from neighbor list, and sends it to all neighbors of A, an authenticated (using shared key) alert message indicating A is a suspected malicious node. When neighbor d_i gets alert, it verifies its authenticity, that α is a first-hop neighbor of A, and that A is d_i's neighbor. It then stores α identity in an alert buffer associated with A. When d_i gets enough alert messages about A, it marks status of A as revoked in neighbor list.

Determination of first and second hop neighbors is important in detecting wormhole attack using local monitoring. A node does not accept/send packets to another node not recognized as a first-hop neighbor. A node acts as guard depending on knowledge of one hop neighbors. Second hop neighbor information detects when a node falsifies information about immediate sender. In a static scenario, neighbor list is built once during deployment when network is assumed adversary-free. But, in a mobile scenario, neighborhood changes during network life and so dynamic secure neighbor discovery is needed. Neighbor determination problem is a subset of verifying location of nodes in two transmission ranges.

A distributed and adaptive statistical profiling technique is proposed to filter RREQs (by destination) or RREPs (by source) with excessively large delays. As

different RREQs take varying number of hops, upper bound is calculated on per hop RREQ/RREP packets time so that normal packets are retained and falsified packets filtered. Retransmit timeout (RTO) calculations used by TCP, that capture average and deviation of round trip times of a connection are calculated. A destination node filters (discards) RREQs targeted to it in this design having excessively large delays. Consider a route discovery from source *S* to destination *D*. *D* receives first copy of RREQ with hop count h_1 at local time t_1, and second copy of RREQ with hop count h_2 at time $t_{2..}$ Let t_0 denote destination local time when request originated at source. As actual value of t_0 is not known, how *D* estimates it is seen below. First RREQ with new sequence number is considered legitimate and destination sends a RREP back to source [38]. For every duplicate RREQ received, destination calculates route request hop time (RHT), time taken by request packet to reach destination divided by its hop count as seen in Equation (1). Destination computes smoothed average, denoted *avgRHT*, and deviation, *devRHT*, of RHT for accepted RREQs, as given in Equation (2) and Equation (3). To distinguish between malicious route requests and normal a cut-off request hop time, *cutoffRHT*, as given in Equation (4) is calculated. For every duplicate RREQ received, a corresponding reply is generated and *avgRHT*and *cutoffRHT*are updated only when this RREQ's RHT is below*cutoffRHT*. Every destination maintains separate *avgRHT*and *devRHT*values for all sources.

$$RHT_i = \frac{t_i - t_0}{h_i} \quad (1)$$

$$diff_i = RHT_i - avgRHT$$

$$avgRHT = avgRHT + \delta \times diff_i \quad (2)$$

$$devRHT = devRHT + \mu \times |diff_i| - devRHT \quad (3)$$

$$cutoffRHT = avgRHT + \phi \times devRHT \quad (4)$$

Various values were experimented with, $\frac{1}{2}, \frac{1}{4}$ *and* $\frac{1}{8}$, for δ and μ and found that $\frac{1}{8}$ is best for both parameters. Assuming that *devRHT* approximatesstandard deviation of sample RHTs, by a law of large numbers in statistics, fewer than 5% of normal requests have RHTs above *cutoffRHT* calculated with $\emptyset$= 2. Next, the issue that destination does not know actual value of t_0 , is addressed along with local time when route discovery was launched.

Trust is computed by

Trust=α* direct trust+β* indirect trust

In this work, parameter α and β are assigned equal weightage of 0.5.

3.4 Reputation

Reputation of node s_j is maintained at node s_i at anytime t is defined as:

$$R_{s_{ij}}^{t} = \frac{\Gamma(v+\omega)}{\Gamma(v)\Gamma(\omega)} p^{v}(1-p)^{\omega}, \quad where\ 0 \le p \le 1, v > 0, \omega > 0$$

$$setting\ v = c_{s_{ij}}^{t} + 1\ and$$

$$\omega = d_{s_{ij}}^{t} + 1, where\ c_{s_{ij}}^{t}, d_{s_{ij}}^{t} > 0$$

Given reputation, $\boldsymbol{R_{s_{ij}}^{t}}$, between two nodes $s_i$ands_j, the reputation q time later, $\boldsymbol{R_{s_{ij}}^{(t+q)}}$, where q>0 , is obtained by incorporating successful interactions $\boldsymbol{c_{s_{ij}}^{(t+q)-t}}$ and unsuccessful interactions $\boldsymbol{d_{s_{ij}}^{(t+q)-t}}$ during period t to $t + q$ as follows [39]:

$$c_{s_{ij}}^{t+q} = c_{s_{ij}}^{t} + c_{s_{ij}}^{(t+q)-t}, d_{s_{ij}}^{t+q} = d_{s_{ij}}^{t} + d_{s_{ij}}^{(t+q)-t}$$

$$R_{s_{ij}}^{t+q} = Beta(c_{s_{ij}}^{t+q} + 1, d_{s_{ij}}^{t+q} + 1)$$

4. EXPERIMENTAL RESULTS

Proposed trust based AOMDV routing protocol is evaluated and compared with AOMDV for the network performance under wormhole attack. The simulations are carried out with 10% and 20% of the nodes being malicious. The simulations are carried for varying number of nodes in the network (25 to 125). The figure 2 to 5 shows Packet Delivery ration, end to end delay, average number of hops and percentage of maliciousness detected respectively.

Table 1 Packet Delivery Ratio

Number of nodes	AOMDV with 10%malicious node	AOMDV with 20% malicious node	Proposed Trust model 10% malicious node	Proposed Trust model 20% malicious node
25	0.7118	0.6845	0.8366	0.8222
50	0.668	0.6467	0.7968	0.7865
75	0.6574	0.6417	0.7938	0.7665

100	0.6264	0.6127	0.7515	0.7357
125	0.5864	0.5718	0.6867	0.676

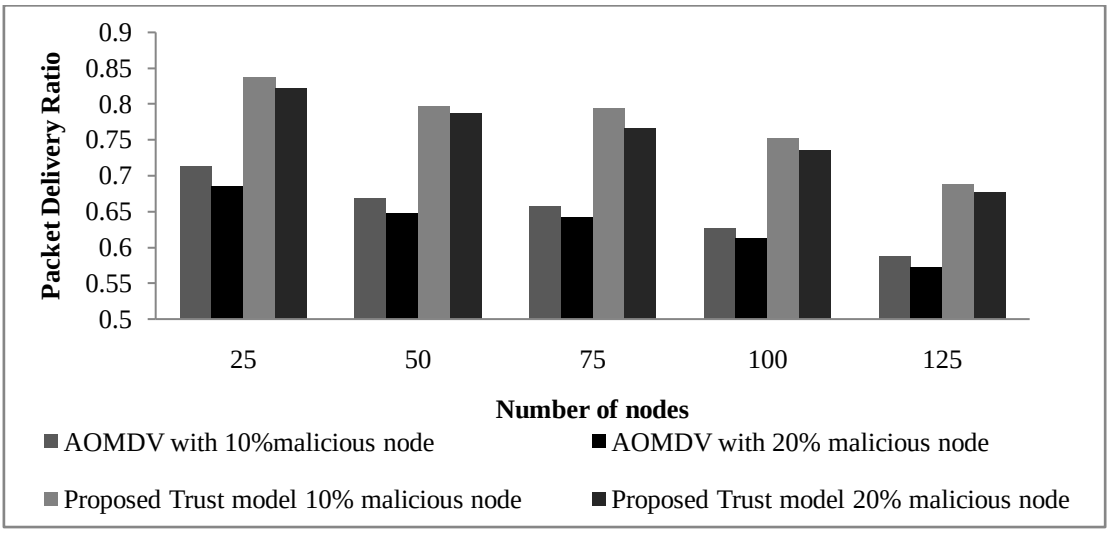

Figure 2 PacketDelivery Ratio

When number of nodes is 75, the proposed method with 10% of malicious nodes improved packet delivery ratio by 18.8% when compared to AOMDV with 10% malicious nodes.When number of nodes is 50, the proposed method with 20% of malicious nodes improved packet delivery ratio by19.51% when compared with AOMDV with 20% malicious nodes.

Table 2 End to End delay

Number of nodes	AOMDV with 10%malicious node	AOMDV with 20% malicious node	Proposed Trust model 10% malicious node	Proposed Trust model 20% malicious node
25	0.0012	0.0012	0.0008	0.001
50	0.0016	0.0014	0.001	0.0012
75	0.0033	0.0016	0.0012	0.0026
100	0.0049	0.0017	0.0012	0.0039
125	0.0153	0.0102	0.0073	0.012

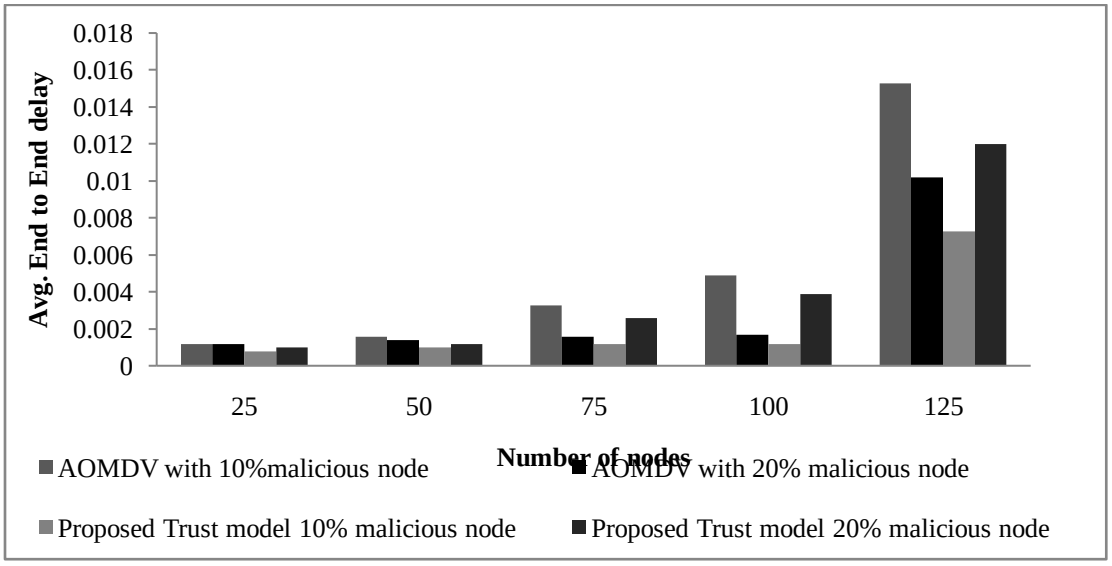

Figure 3 End to End delay

When number of nodes is 75, the proposed method with 10% of malicious nodes decreased end to end delay by 93.33% when compared to AOMDV with 10% malicious nodes. When number of nodes is 50, the proposed method with 20% of malicious nodes decreased end to end delay by 47.62% when compared with AOMDV with 20% malicious nodes.

Table 3 No.of hops to sink

Number of nodes	AOMDV with 10% malicious node	AOMDV with 20% malicious node	Proposed Trust model 10% malicious node	Proposed Trust model 20% malicious node
25	4.2	4.6	3.8	3.5
50	5.7	6	4.8	4.9
75	6.5	6.5	4.9	5.1
100	6.9	6.9	5.3	5.5
125	7.5	7.2	5.3	6

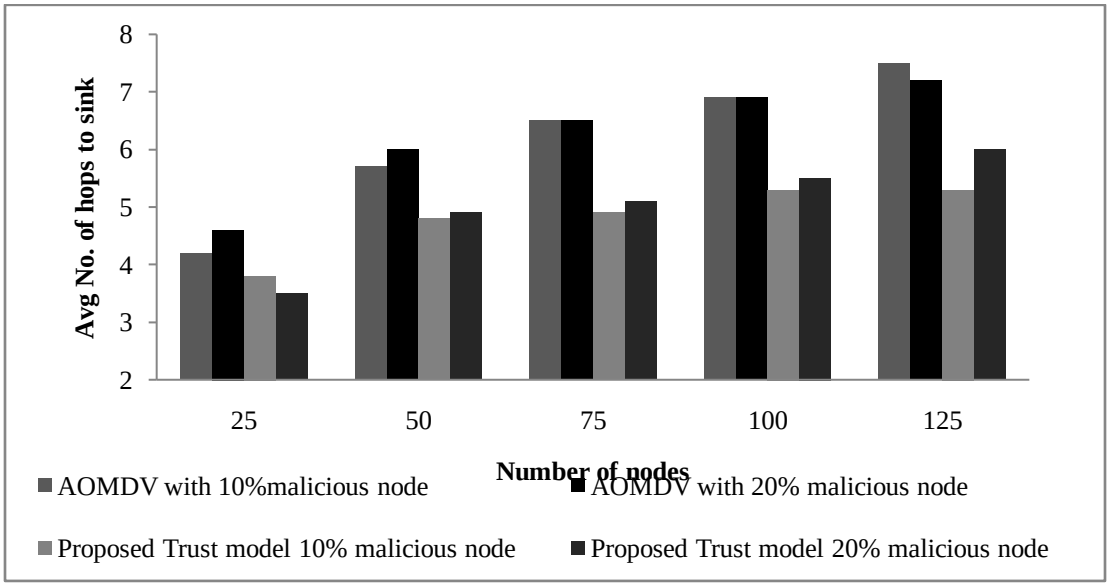

Figure 4 No. of hops to sink

When number of nodes is 75, the proposed method with 10% of malicious nodes decreased number of hops to sink by 28.07% when compared to AOMDV with 10% malicious nodes. When number of nodes is 50, the proposed method with 20% of malicious nodes decreased number of hops to sink by 24.14% when compared with AOMDV with 20% malicious nodes.

Table 4 Percentage of Malicious node detected

Number of nodes	Proposed Trust model 10% malicious node	Proposed Trust model 20% malicious node
25	87	88
50	82	78
75	80	77
100	76	71
125	71	65

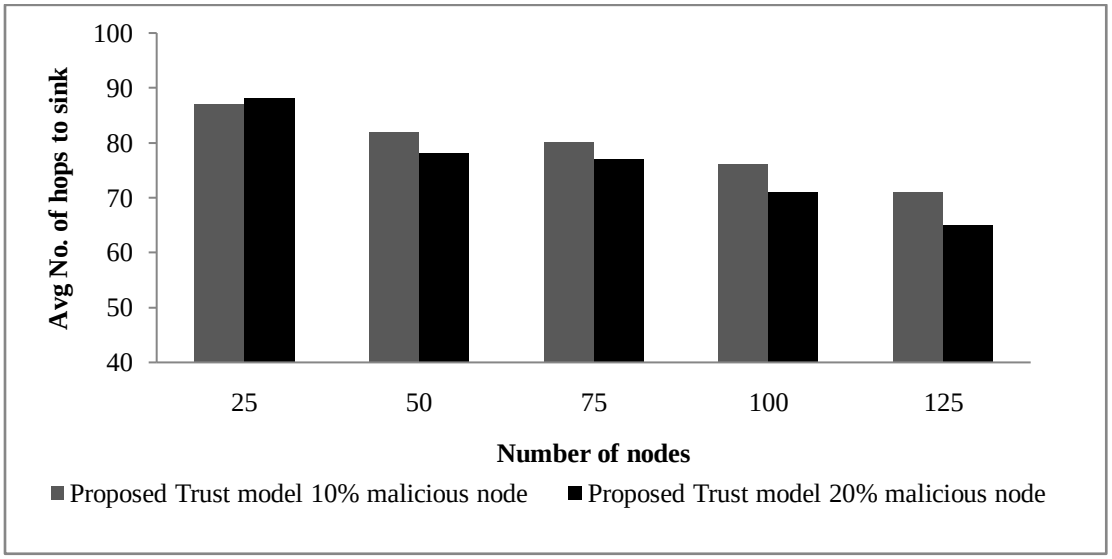

Figure 5Percentage of Malicious node detected

It is observed that as the network size increases, the detection rate of the malicious node is reduced. Further investigations are required to improve the detection rate.

5. CONCLUSION

Network performance and reliability is compromised by attacks on adhoc network routing protocols. In wormhole attacks an intruder makes a tunnel during data transmission from one network end-point to the other, making distant network nodes believe they are with immediate neighbors' and communicate through wormhole link. Experiments were conducted and compared with AOMDV in this study. A distributed and adaptive statistical profiling technique is proposed to filter RREQs or RREPs with excessively large delays. Results revealed that when number of nodes is 75, the proposed method with 10% of malicious nodes improved packet delivery ratio by 18.8% when compared to AOMDV with 10% malicious nodes.

REFERENCES

1. Mueller, S., Tsang, R. P., & Ghosal, D. (2004). Multipath routing in mobile ad hoc networks: Issues and challenges. In *Performance tools and applications to networked systems* (pp. 209-234). Springer Berlin Heidelberg.
2. Sumyla, D. (2006). *Mobile Ad-hoc Networks (manets)*. Technical Report.
3. Royer, E. M., & Toh, C. K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. *Personal Communications, IEEE*, *6*(2), 46-55.
4. Singh, J., & Sharma, S. A survey on routing protocol in MANET.

5. Wu, K., & Harms, J. (2001). Performance study of a multipath routing method for wireless mobile ad hoc networks. In *Modeling, analysis and simulation of computer and telecommunication systems, 2001. Proceedings. Ninth International Symposium on* (pp. 99-107). IEEE.
6. Kaur, R., Mahajan, R., & Singh, A. A survey on multipath routing protocols for MANETs.
7. Stallings, W. Cryptography and network security, principles and practices, 2003. *Practice Hall*.
8. Rai, P., & Singh, S. (2010). A Review of 'MANET's Security Aspects and Challenges'. *International Journal of Computer Applications IJCA*, *4*, 162-166.
9. Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: Vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management*, *11*(2011), 32-37.
10. Yadav, S., Jain, R., & Faisal, M. Attacks in MANET.
11. Ngadi, M., Khokhar, R. H., & Mandala, S. (2008). A review current routing attacks in mobile ad-hoc networks. *International Journal of Computer Science and Security*, *2*(3), 18-29.
12. Jarvenpaa, S. L., Knoll, K., & Leidner, D. E. (1998). Is anybody out there? Antecedents of trust in global virtual teams. *Journal of management information systems*, 29-64.
13. Weick, K. E., & Roberts, K. H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. Administrative science quarterly, 357-381.
14. England, P., Shi, Q., Askwith, B., & Bouhafs, F. (2012). A Survey of Trust Management in Mobile Ad-Hoc Networks. In Proceedings of the 13th annual post graduate symposium on the convergence of telecommunications, networking, and broadcasting, PGNET.
15. Azzedin, F., & Maheswaran, M. (2002). Evolving and managing trust in grid computing systems. In Electrical and Computer Engineering, 2002. IEEE CCECE 2002. Canadian Conference on (Vol. 3, pp. 1424-1429). IEEE.
16. Sen, J. (2010). A distributed trust and reputation framework for mobile ad hoc networks. In Recent Trends in Network Security and Applications (pp. 538-547). Springer Berlin Heidelberg.
17. Kute, V. B., & Kharat, M. U. (2012). Analysis of Quality of Service for the AOMDV Routing Protocol. Engineering, Technology & Applied Science Research, 3(1), pp-359.
18. Sharma, P. (2012). Trust based secure aodv in manet. Journal of Global Research in Computer Science, 3(6), 107-114.

19. Li, W., Joshi, A., & Finin, T. (2010, May). Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach. In Mobile Data Management (MDM), 2010 Eleventh International Conference on (pp. 85-94). IEEE.
20. Agrawal, S., Jain, S., & Sharma, S. (2011). A survey of routing attacks and security measures in mobile ad-hoc networks. arXiv preprint arXiv:1105.5623.
21. Subramanian, S., & Ramachandran, B. (2012). Trust Based Scheme for QoS Assurance in Mobile Ad-Hoc Networks. arXiv preprint arXiv:1202.1664.
22. Ferdous, R., Muthukkumarasamy, V., & Sattar, A. (2010, April). Trust formalization in mobile ad-hoc networks. In Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on (pp. 351-356). IEEE.
23. Jhaveri, R. H., Patel, A. D., Parmar, J. D., & Shah, B. I. (2010). MANET routing protocols and wormhole attack against AODV. International Journal of Computer Science and Network Security, 10(4), 12-18.
24. Balakrishna, R., Rao, U. R., & Geethanjali, N. (2010). Performance issues on AODV and AOMDV for MANETS. International Journal of Computer Science and Information Technologies, 1(2), 38-43.
25. Maulik, R., & Chaki, N. (2011). A study on wormhole attacks in MANET.International Journal of Computer Information Systems and Industrial Management Applications ISSN, 2150-7988.
26. Panaousis, E. A., Nazaryan, L., & Politis, C. (2009, September). Securing AODV against wormhole attacks in emergency MANET multimedia communications. In Proceedings of the 5th International ICST Mobile Multimedia Communications Conference (p. 34). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
27. Cho, J. H., Swami, A., & Chen, R. (2011). A survey on trust management for mobile ad hoc networks. Communications Surveys & Tutorials, IEEE, 13(4), 562-583.
28. Murali, L., & Divya, T. V. Impact of link breaks on AODV and AOMDV in MANET: A Performance Analysis. International Journal of Electronics and Computer Science Engineering (IJECSE), ISSN 2277-1956/V2N1-148, 153.
29. AlMobaideen, W. (2009). SPDA: stability based partially disjoint AOMDV.European Journal of Scientific Research, 27(3), 342-348.
30. Kumar, S., & Parthipan, V. (2011, April). SOPE: Self-organized protocol for evaluating trust in MANET using Eigen Trust Algorithm. In Electronics Computer Technology (ICECT), 2011 3rd International Conference on (Vol. 2, pp. 155-159). IEEE.

31. Mahajan, V., Natu, M., & Sethi, A. (2008, November). Analysis of wormhole intrusion attacks in MANETS. In *Military Communications Conference, 2008. MILCOM 2008. IEEE* (pp. 1-7). IEEE.
32. Marina, M. K., & Das, S. R. (2001, November). On-demand multipath distance vector routing in ad hoc networks. In Network Protocols, 2001. Ninth International Conference on (pp. 14-23). IEEE.
33. Trung, H. D., Benjapolakul, W., & Duc, P. M. (2007). Performance evaluation and comparison of different ad hoc routing protocols. Computer Communications, 30(11), 2478-2496.
34. Sivakumar, K., MCA, M., & Selvaraj, G. (2013). Analysis of Worm Hole Attack In MANET And Avoidance Using Robust Secure Routing Method. International Journal of Advanced Research in Computer Science and Software Engineering,3(1).
35. Blaze, M., Feigenbaum, J., & Lacy, J. (1996, May). Decentralized trust management. In Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on (pp. 164-173). IEEE.
36. Pirzada, A. A., & McDonald, C. (2006). Trust establishment in pure ad-hoc networks. Wireless Personal Communications, 37(1-2), 139-168.
37. Khalil, I., Bagchi, S., & Shroff, N. B. (2008). MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks. *Ad Hoc Networks*, *6*(3), 344-362.
38. Su, X., & Boppana, R. V. (2007, June). On mitigating in-band wormhole attacks in mobile ad hoc networks. In *Communications, 2007. ICC'07. IEEE International Conference on* (pp. 1136-1141). IEEE.
39. Crosby, G. V., & Pissinou, N. (2007, January). Cluster-based reputation and trust for wireless sensor networks. In *Consumer Communications and Networking Conference*.