Trusty DSR Protocol for MANET To Mitigate BLACKHOLE Attacks

Mahamuni, K.
Research Scholar, Department Of Computer Science, Periyar University, Salem-11, Tamil Nadu, India.

Dr. C. Chandrasekar
Professor, Department Of Computer Science, Periyar University, Salem-11, Tamil Nadu, India.

Abstract
Mobile Ad hoc Networks (MANETs) are autonomous mobile node systems connected by wireless links. A node operates as an end system and as a router, to forward packets. MANET routing is challenging and has received tremendous attention from researchers. Dynamic Source Routing (DSR) protocol was accepted as a dominant routing protocol for MANETs. Performance analysis and results show that DSR as an outstanding routing protocol consistently outperforming other routing protocols. This study proposes a new, secure DSR protocol for MANETs based on trust and reputation to mitigate black hole attacks.

Keywords: Mobile Adhoc Network (MANET), Dynamic Source Routing (DSR), Routing, Attacks in MANET, Trust Model

Introduction
MANETs are a group of wireless mobile computers (nodes); where nodes collaborate and forward packets for each other to allow communication outside the range of direct wireless transmissions. Ad hoc networks need no centralized administration/fixed network infrastructure like base stations/access points. MANETs are autonomous mobile users groups communicating over slow wireless links [1]. MANETs with more nodes need more processing power, memory and bandwidth to ensure accurate routing information; this introduces traffic overhead into networks as nodes communicate routing information which also uses up battery power [2].

A MANET is an infrastructure less, self-organized, and multi-hop network having quickly changing topology that causes wireless links to be broken and rebuilt on-the-fly. A key issue is that Routing Protocols must respond rapidly to network topological changes. MANET routing was an active research area and recently numerous protocols were introduced to address routing issues. These protocols are divided into Reactive and Proactive [1] protocols. MANETs offer advantages over conventional networks including reduced infrastructure costs, easy establishment and fault tolerance, as routing is done individually by nodes using intermediate network nodes to forward packets which in turn reduces bottlenecks. But the key MANET attraction is greater mobility compared to wired solutions. There are many issues that affect Ad-hoc networks reliability and limit their viability for varied scenarios; lack of centralised structure in MANETs requires that individual nodes must act as router and be responsible for packet routing tasks; this is done using one/more common routing protocols across MANETs [2].

Security is essential for wired/wireless network communications. MANETs success depends on its security. But, MANETs characteristics pose challenges/opportunities to achieve security goals, like authentication, confidentiality, availability, integrity, access control and non-repudiation. An overview of attacks according to protocols stacks and security attributes and mechanisms is added.

Different Types of Attacks Faced by Routing Protocols
There are various attacks that target the MANETs weakness. Routing messages are essential components of mobile network communications, as a packet needs to be passed via intermediate nodes, which it traverses from the source to destination. There are also other severe attacks in MANET networks possible against routing protocols like AODV and DSR [6].

- **Wormhole Attack**: this is a severe attack where an attacker introduces two malicious nodes in a network; where an attacker forward packets through a private — tunnel.
- **Black-hole attack**: This attack is described well; here a
node advertises a zero metric to destinations, which become a cause to nodes around it to route data packets to it. AODV protocol is vulnerable to such attacks due to having a centric network property, where a network node shares routing tables with each other.

As Black hole attack tries to drop packets instead of forwarding it to its destination or consumes intercepted packet silently, it becomes a very dangerous Denial of Service (DoS) attack for a network. The attack’s effect is based on the type of protocol used by a network. Here, network parameters performance is evaluated with the implementation of varied black hole nodes. Also, performance is evaluated by varying pause time and different node speeds with the implementation of black hole nodes [7].

This Trust-based Multipath Routing (TMR) ensures a method of message security. Less trusted nodes in this approach are given a message’s lesser self-encrypted parts thereby making it difficult for malicious nodes to access minimum information needed to break through the encryption strategy. Trust routing protocols should identify trustworthy nodes and locate a reliable/trustworthy route from sender to destination node within a few seconds or better still in a tenth of seconds, depending on nodes mobility and the hops on the route. Trust based routing protects messages against modification [8]. Trust evaluation in every network node- according to a new solution - was based on parameters like node stability defined by mobility/pause time and remaining battery power. Node trust is the basis for selection of a reliable transmission route [9].

A node stops for a duration defined by ‘pause time’ parameter when it reaches a destination. After pause time, it chooses a random destination again and repeats the process till simulation ends [29]. Time taken by a node to choose a destination for packet delivery is ‘pause time’. Trust is important in MANET routing. So a new, secure DSR protocol for MANETs based on trust/reputation is proposed to offset black hole attacks. Communication nodes selection is based on a reputation based trust mechanism. Section 2 deals with literature related to this work, section 3 reveals methods used in this work, section 4 deals with results and discussion of the obtained results and finally Section 5 concludes the work.

**Literature Review**

A MANET routing protocol that enabled efficient usage of power/bandwidth in MANETs was proposed by Durai & Baskaran [10]. Randomized Overhearing techniques were proposed to reduce power consumption and enhance effective MANET routing. Randomized overhearing technique with AODV/DSR protocols reduced power consumed during transmission in MANETs. Minimum hop path to reduce excess bandwidth consumption was suggested. Mediation Device (MD) protocol to extend nodes battery life in a MANET scenario was introduced.

Conventional DSR and Destination-Sequenced Distance-Vector Routing (DSDV) routing protocol to improve DSR routing protocol using Time to Live (TTL)-based scheme investigated by Tambuwal et al., [11] showed that DSDV outperformed DSR specially when nodes moved at high speed, due to DSR’s inability to repair broken links locally and also due to lack of a mechanism to control route freshness when there were multiple options. A new mechanism, DSR_TTL was proposed to improve conventional DSR performance. Results have showed that the new protocol improved network throughput and total reduced overhead.

The power consumption aspect of MANET routing protocols was discussed by Barati et al., [12]. Performance comparison of DSR/AODV routing protocols with regards to average energy consumption and routing energy were explained. An evaluation of how different metrics in diverse scenarios affect both protocols power consumption was discussed. A detailed simulation model using NS2 with different mobility/traffic models was used for energy consumption. An energy consumption based evaluation of routing protocols was presented.

A 'voting' mechanism to access recommending the experience (ratings) to reduce algorithm design cost and system overhead was introduced by Xia et al., [13]. Then a novel Trust-enhanced Multicast Routing protocol (TeMR) combined with a trust model was proposed. The new protocol introduced a group-shared tree strategy that establishes efficient multicast routes as it used ‘trust’ to improve the forwarding tree’s efficiency and robustness. Is also provided a flexible/feasible approach to routing decision with trust constraint / malicious node detection. Experiments evaluated the new protocol’s effectiveness.

An energy consumption model to calculate nodes energy-factor introduced by Sarkar & Datta [14] proposed a trust based protocol for energy-efficient routing. A trusted module to track routing metric valued was adopted. The simulation showed that the new protocol reduced delay, routing overhead, and increased packet delivery ratio by consuming less energy compared to AODV and DSRs.

Trust based Ad hoc On-Demand Routing protocol for MANETs was presented by Gupta & Pandey [15]. The authors proposed algorithm works on the concept of honest value calculated on a concept of hop/trust to protect networks from malicious nodes. The proposed protocol’s performance was analysed using throughput, dropped packets, packet delivery ratio and received packets with varied number of nodes, speed and simulation time. Results showed that the new method had better performance and enhanced network security.

A Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs was proposed by Aggarwal et al., [16]. AODV routing protocol was modified to implement TSDRP to make it secure against attacks like Blackhole and DOS attacks. To evaluate performance, Packet Delivery Fraction (PDF), Average Throughput (AT) and Normalized Routing Load (NRL) were considered.

A MANET trust management scheme was proposed by Rahman [17], where trust value was used to establish a communication link between a node that initiates communication (initiator node) and a destination node. Graph theoretic approach was used in the new scheme to locate a path and both direct trust and neighbouring nodes recommendations were used to compute trusted communication path. The highest trusted but minimum routing path was achieved from initiator node to a destination node by this scheme. Trust management scheme can be included in efficient routing algorithms to achieve highest trusted but minimum routing path from initiator
nodes to destination nodes.
A routing algorithm which adds a field in request packet storing trust value indicating node trust on neighbours proposed by Mangrulkar & Atique [18] was based on level of trust factor, routing information being transmitted depending on highest trust value among all. A malicious node could attack a control packet and misbehave in a network. The malicious node may/may not be a trusted node. In the new work, trusted path used irrespective of shortest/longest path is used for network communication.

A new scheme, Administrator and Trust Based Secure Routing (ATSR) in MANET proposed by Banerjee et al., [19] provided routing by using a parameter, trust, an integer value, and selecting the administrator inside a network for routing. Message confidentiality/integrity was implemented. Simulation showed the new routing scheme’s efficiency, lustiness and trustworthiness.
Routing protocols used in MANET, DSDV, DSR and AODV routing protocols are simulated using different scenarios regarding different Traffic types, Constant Bit Rate (CBR), Variable Bit Rate (VBR) concentrated on by Razouqi et al., [20] combined both classes in one scenario to scrutinize the combination’s impact. Routing protocols were analysed against performance metrics, PDF, Average energy consumption, NRL, Average throughput and Total Dropped Packets (TDP). Traffic results combined pronounced that DSR/AODV show better behaviour overall in the performance metrics examined.
An optimized method for an optimal path between a pair of nodes to detect misbehaving (selfish, incapable) nodes in MANETs was described by Varshney et al., [21]. This improved routing protocol performance as in most poor performing networks, misbehaving nodes are the cause. DSR protocol was deployed (using NS2 simulator) followed by application of Genetic Algorithm to detect selfish nodes to find an optimal path between a pair of nodes. Misbehaving node(s) were successfully detected proving that the new approach was optimal and improved DSR performance significantly.

Two MANET protocols (AODV/DSR) were inspected/examined for their performance by Anjmad & Stocker [22] based on node density variation and mobility using mobility models like Random Way Point (RWP) and Random Way Point with Attractions (RWP-ATTR). Performance was determined based on normalized routing load, packet delivery ratio, throughput and average end-to-end delay with varying node densities/mobility. DSR with higher node density showed extreme performance degradation. Non-uniform node distribution for RWP significantly impacted performance results in both protocols.

Methodology
This section discusses DSR and the proposed trust model.

Dynamic Source Routing (DSR):
DSR is an efficient routing protocol designed for multi-hop wireless ad hoc mobile networks. It is an important routing protocol used in MANETs as energy efficient routing protocols are designed based on mechanism. It finds a route from source to destination only when a source initiates route discovery. The protocol totally operates on demand making the network self-organizing and self-configuring. The protocol is composed of Route Discovery and Route Maintenance mechanisms which work together to allow nodes discover/maintain source route to a destination node in ad hoc networks [23].

- Route Discovery
- Route Maintenance

Route Discovery is when a node S wishing to send a packet to a destination node D gets a source route to D. Route Discovery is used only when S starts to send a packet to D and does not know a route to D already.
Route Maintenance is a mechanism where node S detects, while using a source route to D, as to whether network topology had changed so that it can no longer use the route to D as a link on the route does not work. When Route Maintenance reveals a source route is broken, S attempts to use any other route it knows to D, or invokes Route Discovery again to locate a new route. Route Maintenance is used when S actually sends packets to D.
Route Discovery/Route Maintenance operate on demand. Unlike other protocols, DSR needs no periodic packets at any level within a network. DSR does not use periodic routing advertisement, link status sensing, or neighbour detection packets. It also does not rely on these functions from any underlying network protocols.
DSR’s on-demand behaviour and lack of periodic activity allows many overhead packets to scale down to zero, when nodes are approximately stationary regarding each other and routes needed for current communication are already discovered. As nodes move more or as communication patterns change, DSR routing packet overhead automatically scales to only that needed to track routes in use [24].
All data packets sent using DSR protocol contain a complete nodes list that a packet has to traverse. During route discovery, source node broadcasts a ROUTE REQUEST (RREQ) packet having a unique identification number. The RREQ has the target node’s address to which the route is desired. All nodes without information regarding target node, or have not seen the same RREQ packet earlier, append their IP addresses to it and rebroadcast it.
To control spread of RREQ packets, the broadcast is done in a non-propagating manner with IP TTL field being incremented in a route discovery. ROUTE REQUEST packets keep spreading in a network till they reach a target node or any other node with a target node route. The recipient node creates a ROUTE REPLY packet, with a complete list of nodes that RREQ packet traversed. Based on the implementation, a target node may respond to one/more incoming ROUTE REQUEST packets. Similarly, a source node may accept one/more ROUTE REPLY packets for one target node [25].
When a data link layer detects a link disconnection in DSR, a ROUTE_ERROR packet is reverted to the source. On receipt of the ROUTE_ERROR packet, source node initiates another route discovery operation. Also routes containing a broken link are removed from route caches of immediate nodes when a ROUTE_ERROR packet is transmitted to source [26].
Proposed Trust Model:
Nodes using trust models, measure neighbors accuracy and authenticity through monitoring of their packet forwarding participation. A sending node verifies a source route header’s different fields in forwarded IP packets for modifications via integrity checks. If successful, it ensures that a node behaved benevolently and hence its direct trust counter increases. But, if forwarding node fails to transmit packet or if the integrity check fails then its direct trust measure decreases [27].

Trust is measured through recourse to three scenarios likely to be based on data packets forwarded, control packets forwarded and routing protocol execution. Based on the behavior of these, attacks are addressed. The Data message/packet forwarding based trust are effectively used for addressing Black-hole, sinkhole, selective forwarding, denial of service and selfish behavior. The control message forwarding metric helps in Control and routing message dropping attacks. The routing protocol’s specific actions (reaction to specific routing messages) mitigate misbehavior related to particular routing protocol actions.

A node’s direct trust is used in an effort-return based trust model. Immediate neighbouring nodes sincerity and trust is measured by observing their contribution to packet forwarding. Every time a node transmits data/control packet it immediately brings its receiver to a promiscuous mode, to overhear its immediate neighbour forwarding a packet.

A sending node verifies different fields in a forwarded IP packet for necessary modifications through integrity checks. If they succeed, it confirms that a node has acted benevolently and so its direct trust counter is incremented. Similarly, if the integrity check fails or a forwarding node does not transmit a packet at all, its direct trust measure is decremented.

Direct trust in a node y by node x as $T_{xy}$ is given by the equation (1):

$$T_{xy} = W(P_A) \times P_A + W(P_p) \times P_p$$

Where $P_A$ represents category Packet Acknowledgements that preserves a count of packets forwarded by a node. $P_p$ represents category Packet Precision, which maintains a count of packets forwarded correctly. $W$ reflects weight/priority assigned to a particular category. Category $P_A$ and $P_p$ are used in combination to protect DSR protocol against deceptive alteration of vital protocol fields and to identify selfish node behaviour respectively [25].

In trust model, a node i (deciding node) maintains three kinds of ratings about neighbouring node j (suspect node). In the scheme, a node calculates cooperation score $C_{ij}$ and direct trust value $T_{ij}^D$ according to a distribution (called “prior”) updated as soon as new observations are made, and a reported rating from neighbouring nodes (indirect trust value $T_{ij}^I$).

These three ratings are used to calculate overall trust value $T_{ij}$.

Computing direct trust value and cooperation score are based on a statistical updating (positive rating; $\alpha$, or negative rating; $\beta$) of beta probability density function. Probability density function of overall trust value $T$ on interval (0, 1), is represented to have a Beta distribution as in equation (2):

$$f(T|\alpha,\beta) = \frac{r(\alpha)}{r(\alpha)r(\beta)}T^{\alpha-1}(1-T)^{\beta-1}$$

Where $\alpha$ is the positive trust rating ($\alpha > 0$), with initial value = $1$ $\beta$: is the negative trust rating ($\beta > 0$), with initial value = $1$ $T$: is the trust value $0 \leq T \leq 1$

$f = \alpha + \beta$, is the certainty factor where the larger the sum ($\alpha + \beta$), the more certainty about the trust value [28].

Consider interaction of two nodes $s_i$ and $s_j$, from perspective of $s_i$ there are two possible outcomes $O_{s_i} = 1$ for successful interaction and $O_{s_i} = 0$ for unsuccessful interaction. In this context $c_i^t$, $d_i^t$, which are defined previously also mean that the outcome $O_{s_i} = 1$ is observed $c_i^t$ times and $O_{s_i} = 0$ is observed to occur $d_i^t$ times. The probability density function of observing outcome $O_{s_i} = 1$ in future can be expressed as a function of past observations by equation (3):

$$v = c_i^t + 1 \text{ and } \omega = d_i^t + 1, \text{ where } c_i^t, d_i^t \geq 0$$

The expectation value for the beta distribution is defined as:

$$E(p) = \frac{\sqrt{v}}{\sqrt{v + \omega}}$$

where $p$ is probability variable.

Reputation of node $s_i$ that is maintained at node $s_j$ at any time t is defined as in equation (4):

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

setting $v = c_i^t + 1$ and $\omega = d_i^t + 1$, where $c_i^t, d_i^t \geq 0$ Given reputation, $R_{ij}^t$ between two nodes $s_i$ and $s_j$, reputation $q$ time later, $R_{ij}^{(t+q)}$, where $q > 0$, is obtained by incorporating number of successful interactions $c_{ij}^{t+q}$ and number of unsuccessful interactions $d_{ij}^{t+q}$ during period $t$ to $t+q$ as in equation (5):

$$c_{ij}^{t+q} = c_i^t + c_{ij}^{t+q-1}, d_{ij}^{t+q} = d_i^t + d_{ij}^{t+q-1}$$

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

Pseudo code of the proposed method:
Procedure Trust ();// compute trust in nodes // Updates trust values in all nodes
1. Nodes compute Direct Trust
   $$T_{xy} = W(P_A) \times P_A + W(P_p) \times P_p$$
2. Compute Reputation
   $$R_{xy}^{(t+q)} = Beta(c_{xy}^{t+q} + 1, d_{xy}^{t+q} + 1)$$
3. Update trust values in routing table
//Route Discovery//
1. Source node sends Route_Request
//Update Cache info//
2. Updated trust values in routing table
3. Check trust value
4. If node==destination
   Copy the trust value and most reliable path to Route_Rply
5. If Intermediate node
   Case a. Route to destination in cache: Copy the trust value and most reliable path to Route_Rply
   Case b. No Route to destination in cache: Add address and trust value in Route_Record[] and rebroadcast.

Experimental Results
For experiments, 80 numbers of nodes are used. The area considered is 4 sq. km with different node pause time. Transmission range of node is 200 m. Constant bit rate is used as the data type. DSR Header modification is performed to accommodate trust values in hello message varying in speed with 10% and 20% maliciousness. The experimental results for 10% of malicious nodes are shown in figures 1 to 4 and table 1 to 4 as follows:

Table 1: End to End Delay for 10% malicious nodes

<table>
<thead>
<tr>
<th>Node Pause time (sec)</th>
<th>DSR (sec)</th>
<th>Trust Based DSR (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.061824</td>
<td>0.040161</td>
</tr>
<tr>
<td>10</td>
<td>0.048391</td>
<td>0.033999</td>
</tr>
<tr>
<td>20</td>
<td>0.018201</td>
<td>0.015543</td>
</tr>
<tr>
<td>30</td>
<td>0.014159</td>
<td>0.012389</td>
</tr>
<tr>
<td>40</td>
<td>0.001606</td>
<td>0.001332</td>
</tr>
<tr>
<td>50</td>
<td>0.001282</td>
<td>0.001075</td>
</tr>
</tbody>
</table>

Figure 1: End to End Delay for 10% malicious nodes

The proposed trust based DSR reduced end to end delay by 42.48% as highest value when compared with DSR in 0 node pause time. The proposed trust based DSR reduced end to end delay by 17.56% as least value when compared with DSR in 50 node pause time. Averagely trust based DSR reduced by 32.69% of end to end delay when compared with DSR with 10% of malicious nodes in network.

Table 2: Packet Delivery Ratio for 10% malicious nodes

<table>
<thead>
<tr>
<th>Node Pause time (sec)</th>
<th>DSR(sec)</th>
<th>Trust Based DSR(sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.6781</td>
<td>0.8072</td>
</tr>
<tr>
<td>10</td>
<td>0.7864</td>
<td>0.8123</td>
</tr>
<tr>
<td>20</td>
<td>0.8443</td>
<td>0.8738</td>
</tr>
<tr>
<td>30</td>
<td>0.8839</td>
<td>0.9191</td>
</tr>
<tr>
<td>40</td>
<td>0.8997</td>
<td>0.9479</td>
</tr>
<tr>
<td>50</td>
<td>0.9338</td>
<td>0.9684</td>
</tr>
</tbody>
</table>

Figure 2: Packet Delivery Ratio for 10% malicious nodes

The proposed trust based DSR improved packet delivery ratio by 3.64% as highest value when compared with DSR in 50 node pause time. The proposed trust based DSR improved packet delivery ratio by 17.38% as least value when compared with DSR in 0 node pause time. Averagely trust based DSR improved by 5.84% of packet delivery ratio when compared with DSR with 10% of malicious nodes in network.

Table 3: Number of hops to destination for 10% malicious nodes

<table>
<thead>
<tr>
<th>Node Pause time (sec)</th>
<th>DSR(sec)</th>
<th>Trust Based DSR(sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5.5</td>
<td>5.6</td>
</tr>
<tr>
<td>10</td>
<td>5.3</td>
<td>5.5</td>
</tr>
<tr>
<td>20</td>
<td>4.7</td>
<td>4.9</td>
</tr>
<tr>
<td>30</td>
<td>4.7</td>
<td>4.5</td>
</tr>
<tr>
<td>40</td>
<td>4.3</td>
<td>4.2</td>
</tr>
<tr>
<td>50</td>
<td>3.5</td>
<td>3.7</td>
</tr>
</tbody>
</table>

Figure 3: Number of hops to destination for 10% malicious nodes
The proposed trust based DSR reduced number of hops to destination by 1.80% as highest value when compared with DSR in 0 node pause time. The proposed trust based DSR reduced number of hops to destination by 5.56% as least value when compared with DSR in 50 node pause time. Averagely trust based DSR reduced by 1.42% of number of hops to destination when compared with DSR with 10% of malicious nodes in network.

**Table 4: Packet Loss Rate for 10% malicious nodes**

<table>
<thead>
<tr>
<th>Node Pause time (sec)</th>
<th>DSR(%)</th>
<th>Trust Based DSR(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.3219</td>
<td>0.1928</td>
</tr>
<tr>
<td>10</td>
<td>0.2136</td>
<td>0.1877</td>
</tr>
<tr>
<td>20</td>
<td>0.1557</td>
<td>0.1262</td>
</tr>
<tr>
<td>30</td>
<td>0.1161</td>
<td>0.0809</td>
</tr>
<tr>
<td>40</td>
<td>0.1003</td>
<td>0.0521</td>
</tr>
<tr>
<td>50</td>
<td>0.0662</td>
<td>0.0316</td>
</tr>
</tbody>
</table>

**Figure 4: Packet Loss Rate for 10% malicious nodes**

The proposed trust based DSR reduced Packet loss rate by 50.17% as highest value when compared with DSR in 0 node pause time. The proposed trust based DSR reduced Packet loss rate by 70.76% as least value when compared with DSR in 50 node pause time. Averagely trust based DSR reduced by 36.76% of Packet loss rate when compared with DSR with 10% of malicious nodes in network.

**Figure 5: End to End Delay for 20% malicious nodes**

The proposed trust based DSR reduced end to end delay by 46.04% as highest value when compared with DSR in 0 node pause time. The proposed trust based DSR reduced end to end delay by 11.42% as least value when compared with DSR in 50 node pause time. Averagely trust based DSR reduced by 35.2% of end to end delay when compared with DSR with 20% of malicious nodes in network.

**Table 5: End to End Delay for 20% malicious nodes**

<table>
<thead>
<tr>
<th>Node Pause time (sec)</th>
<th>DSR(sec)</th>
<th>Trust Based DSR(sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.0717</td>
<td>0.001453</td>
</tr>
<tr>
<td>10</td>
<td>0.0558</td>
<td>0.001296</td>
</tr>
<tr>
<td>20</td>
<td>0.0220</td>
<td>0.001504</td>
</tr>
<tr>
<td>30</td>
<td>0.0170</td>
<td>0.001430</td>
</tr>
<tr>
<td>40</td>
<td>0.0019</td>
<td>0.001504</td>
</tr>
<tr>
<td>50</td>
<td>0.0001</td>
<td>0.001504</td>
</tr>
</tbody>
</table>

**Figure 6: Packet Delivery Ratio for 20% malicious nodes**

The proposed trust based DSR improved packet delivery ratio by 5.12% as highest value when compared with DSR in 50 node pause time. The proposed trust based DSR improved packet delivery ratio by 16.2% as least value when compared with DSR in 0 node pause time. Averagely trust based DSR improved by 6.64% of packet delivery ratio when compared with DSR with 20% of malicious nodes in network.
Table 7: Number of hops to destination for 20% malicious nodes

<table>
<thead>
<tr>
<th>Node Pause time (sec)</th>
<th>DSR(sec)</th>
<th>Trust Based DSR(sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5.5</td>
<td>5.6</td>
</tr>
<tr>
<td>10</td>
<td>5.5</td>
<td>5.6</td>
</tr>
<tr>
<td>20</td>
<td>4.9</td>
<td>5.0</td>
</tr>
<tr>
<td>30</td>
<td>4.9</td>
<td>4.7</td>
</tr>
<tr>
<td>40</td>
<td>4.6</td>
<td>4.3</td>
</tr>
<tr>
<td>50</td>
<td>3.9</td>
<td>4.0</td>
</tr>
</tbody>
</table>

Figure 7: Number of hops to destination for 20% malicious nodes

The proposed trust based DSR reduced number of hops to destination by 1.8% as highest value when compared with DSR in 0 node pause time. The proposed trust based DSR reduced number of hops to destination by 2.53% as least value when compared with DSR in 50 node pause time. Averagely trust based DSR reduced by 0.34% of number of hops to destination when compared with DSR with 20% of malicious nodes in network.

Table 8: Packet Loss Rate for 20% malicious nodes

<table>
<thead>
<tr>
<th>Node Pause time (sec)</th>
<th>DSR</th>
<th>Trust Based DSR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.381</td>
<td>0.2719</td>
</tr>
<tr>
<td>10</td>
<td>0.2817</td>
<td>0.2695</td>
</tr>
<tr>
<td>20</td>
<td>0.2406</td>
<td>0.215</td>
</tr>
<tr>
<td>30</td>
<td>0.2321</td>
<td>0.1757</td>
</tr>
<tr>
<td>40</td>
<td>0.1931</td>
<td>0.1311</td>
</tr>
<tr>
<td>50</td>
<td>0.1739</td>
<td>0.1305</td>
</tr>
</tbody>
</table>

Figure 8: Packet Loss Rate for 20% malicious nodes

The proposed trust based DSR reduced Packet loss rate by 33.42% as highest value when compared with DSR in 0 node pause time. The proposed trust based DSR reduced Packet loss rate by 28.52% as least value when compared with DSR in 50 node pause time. Averagely trust based DSR reduced by 22.87% of Packet loss rate when compared with DSR with 20% of malicious nodes in network.

Conclusion

DSR protocol ensures excellent performance for routing in multi-hop wireless ad-hoc networks. The protocol in a real ad-hoc network has very low routing overhead and correctly delivers almost all data packets, even with the nodes continuous, rapid motion in a network. A trust based DSR is proposed and trust evaluation calculated. Experiments are done with 10% and 20% malicious nodes respectively. Trust based DSR improved packet delivery ratio in the experiments and reduces end to end delay and packet loss rate significantly. The hops to destinations are more or less the same with DSR. Results proved that the new method outperformed conventional DSR.

References

analysis of AODV & DSR routing protocol in mobile
Thakare, A. N., and Joshi, M. Y., 2010,
IEEE 13th International Conference on
routing protocol based on node’s behavior assessment
K. (2014,


