Journal of Theoretical and Applied Information Technology
10th July 2015. Vol.77. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TRUST BASED DYNAMIC SOURCE ROUTING PROTOCOL FOR MANET AGAINST ROUTING ATTACKS

[1]K.MAHAMUNI, [2]DR.C.CHANDRASEKAR

[1]Research Scholar, Department Of Computer Science, Periyar University, Salem-11, TamilNadu, India.
[2]Professor, Department Of Computer Science, Periyar University, Salem-11, TamilNadu, India.
E-mail: [1]mahamunik23@gmail.com, [2]ccsekar@gmail.com

ABSTRACT

Devices themselves are the network in adhoc networks allowing seamless communication, at low cost, in a self-organized fashion and also easy deployment. Freedom and self-organizing capabilities make Mobile Adhoc Networks (MANETs) completely different from other networking solution. MANETs highly dynamic nature leads to changes and network topologies unpredictability, adding difficulty and complexity to mobile node routing within the network. This study proposes a new, secure, Dynamic Source Routing (DSR) protocol for MANETs based on trust and reputation to mitigate black hole attack. Trust metric is based on data packets, control packets forwarded and routing protocol execution. Communication nodes are selected based on a reputation based trust mechanism.

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

1. INTRODUCTION

A MANET is a self-configuring mobile routers (and associated hosts) network connected by wireless links – thereby forming a random topology. Routers move freely and randomly, organizing themselves at random; so, a network's wireless topology changes rapidly/unpredictably. Such networks may operate standalone or may be connected to a larger Internet. Minimal configuration and quick deployment suit adhoc networks for emergency situations like natural/human induced disasters, emergency medical situations, military conflicts, etc. [1]. Users' mobile devices in a MANET are the network, and they cooperatively provide functionality, usually provided by network infrastructure (routers, switches, servers). A MANET needs no infrastructure to enable information exchange among users' mobile devices.

MANETs are becoming important as they help realize network services for mobile users in areas without communications infrastructure, or when such infrastructure needs wireless extension [2]. Adhoc nodes can be connected to a fixed backbone network via a dedicated gateway device enabling IP networking services in places where Internet services are not available due to an absence of infrastructure.

A major issue that affects adhoc network performance is how the routing is implemented in a network. Routing algorithms in conventional wired networks are unfeasible in adhoc networks due to its lack of ability to adapt to changing topology in mobile environments [3]**.** Usually, routing is a process of *discovery, selecting,* and *maintaining paths* from source node to destination node to deliver data packets. Every routing algorithm's goal is directing traffic from source to destination, maximizing network performance and lowering costs. This is a challenge in MANET as it has dynamic and random characteristics.

Routing protocols are classified into two classes based on time when routing information is updated as Proactive Routing Protocols and Reactive Routing Protocols [4]. Another routing protocols classification is source routing and hop-by-hop routing. In source routing, source computes complete path to a destination, which leads to loop-free routing. In hop-by-hop routing, every intermediate node computes next hop itself.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DSR is an efficient routing protocol designed for multi-hop wireless adhoc networks. DSR allows a network to be entirely self-organized and self-configured without need for existing network infrastructure/administration. DSR is a reactive routing protocol using source routing to forward packets. It uses source routing, meaning that source must know complete destination hop sequence. DSR's basic operation consists of two operations: Route Discovery and Route Maintenance.

DSR uses Route Error packet and Acknowledgements for route maintenance. When a node has a fatal transmission problem at data link layer, it generates a Route Error packet. On receipt of route error packet, the node removes the hop in error from its route cache. Every route with hop in error is truncated here. Acknowledgment packets verify correct route links operation. This includes passive acknowledgments where a node hears a next hop forwarding a packet along a route [5, 6].

MANET security is most important for basic network functionality. Network services availability, data confidentiality and integrity are achieved by ensuring that security issues are met. MANETs suffer from security attacks as its features like changing topology dynamically, open medium, lack of central monitoring and management, no clear defense mechanism and cooperative algorithms. These factors change battle field situation for MANETs against security threats [7]. MANET's ultimate goal is providing security solutions. To ensure a security solution there are some mechanisms which prevent, detect and respond. They include Confidentiality, Availability, Authentication and Integrity. A brief explanation of these terms follows:

Availability: The network is available only for authenticated users. This mechanism protects against attacks like Gray hole, black hole, Information disclosure and Message altering.

Confidentiality: MANET finds it hard to attain confidentiality due to intermediate nodes routing, which easily retrieve information from routing nodes.

Integrity: Information transmission must be protected against alteration/message modification.

Authentication: Network should be accessed only by authenticated nodes like Digital signature, Reply and Non repudiation [8].

MANET attacks are classified as:

- Passive Attacks
- Active Attacks

A passive attack does not disrupt network operation. An active attack alters/destroys the data exchanged in the network. In passive attacks, attacker sneaks data without touching it. Passive attacks are tough to detect as there is no change in network functionality [9]. Active attacks are internal or external. Internal attacks are by within network nodes while external attacks are by nodes outside a network. Impersonation, modification and fabrication are some common attacks that are security concerns for MANETs. Some attacks are described below [10]:

Eavesdropping

Eavesdropping is an attack that happens in MANETs. It tries to get confidential information that should be secret during communication.

Traffic Analysis and Monitoring

In traffic analysis attack, the adversaries monitor packet transmission to gather important information like source, destination or source-destination pair.

Jamming attack

Jamming is a specific type of DOS attacks. The objective is to interfere with legitimate wireless communications. A jammer achieves this by preventing a real traffic source from sending a packet, or by preventing receipt of legitimate packets.

Wormhole attack

An attacker records packets at one network location, tunneling them to another. Routing is disrupted when routing control messages are tunneled. A tunnel between two colluding attackers is called a wormhole, which are severe threats to MANET routing protocols.

Byzantine attack

In a byzantine attack, a compromised intermediate node works unaided, or a set of compromised intermediate nodes conspire and carry out attacks like forwarding packets through non-optimal paths, creating routing loops, or

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

selectively dropping packets which disrupts/degrades routing services.

Reputation and trust are two tools that facilitate decision making in diverse fields from ancient fish markets to state-of-the-art ecommerce. Reputation is opinion of one entity about another. In an absolute context, it is an entity's trustworthiness [11]. Trust is the expectancy of one entity about another's actions. Trust is an important factor affecting consumer behavior, especially in an e-commerce context where uncertainty exists. Trust is necessary when there is uncertainty.

Trust is complex and multidimensional. Trust mechanism is introduced in protocols to ensure MANET security. Trust is a value based on nodes action when needed. Trust prevents various attacks like black-hole, wormhole, DOS and selfish attacks. Trust is implemented in differing ways like reputation, subjective logic, nodes opinions etc. as trust has no specific definition.

Trust models attempt to formalize trust definitions and are linked to establishment of public key infrastructure in MANETs. A trust management and recommendation protocol is built upon pretty good privacy methods to compute authenticity based on certificates, key bindings, and trust relationships where opinion and evidence driven models represent trust. Trust and Reputation method identifies attack sources and malicious nodes. A node is identified by another through its reliable packet delivery. This makes that node "trustworthy". Reputation is based on past behavior and a node's time. Nodes past behavior is stored in data form in a centralized/distributed way [13].

Trust computation involves assigning weights (utility/importance factor) to events that they monitor and quantify. Weight assignment depends on application type demanding trust. Nodes are dynamically assigned weights based on their criteria and circumstances. Weights have a continuous range from 0 to +1 representing significance of a specific event from unimportant to most important. Trust values for a node's events can be combined using individual weights to determine aggregate trust level for another node [14].

Routing is a major MANET issue. There are many challenges in adhoc network routing. Trust is most important in MANET routing. So a new, secure, Dynamic Source Routing (DSR) protocol for MANETs is proposed based on trust and reputation to offset black hole attacks. Selection of communication nodes is based on a reputation based trust mechanism. Section 2 describes related work and Section 3 explains the methodology. Section 4 discusses experiments and results. Section 5 concludes the paper.

2. LITERATURE REVIEW

A DSR based secure routing protocol named Baited-black-hole DSR (BDSR) was proposed by Tsou et al., [15]. BDSR detected and avoided black hole attacks by merging MANETs proactive and reactive defense architecture using virtual and non-existent destination address to lure malicious node to reply. MANETs dynamic network topology, infrastructure-less property and lack of certificate authority ensure difficult security problems. Current common routing protocols like DSR and AODV consider performance. They don't have related detection and response mechanisms.

An approach to detect black and grayhole attacks in adhoc network established on a cross layer design was demonstrated by Cai et al., [16]. A path-based method was proposed in a network layer to overhear next hop's action. The proposed scheme does not send extra control packets and saves the detecting node's system resources. A collision rate reporting system is established in MAC layer to estimate dynamic detecting threshold to lower false positive rate under high network overload. DSR protocol was selected to test the new algorithm and ns-2 was simulation tool. Results verified the new theory: average detection rate was above 90% and false positive rate below 10%. Also, adaptive threshold strategy contributed to decreasing false positive rate.

A new approach for black hole prevention in DSR based on route caching was proposed by Patil and Bhole [17] where once the black hole node in MANET is detected during path construction, the culprit's id is passed to DSR path function. Here, paths were ready to be added in route cache but, adding each path in route cache was decided by parsing the paths for the black hole node id. This process used normal caching time process only.

A new scheme Detecting Collaborative Blackhole Attacks (DCBA) to detect collaborative black hole attacks in MANETs was introduced by Woungang et al., [18]. Simulation results demonstrated the superiority of DCBA compared to DSR and Bait DSR scheme (BDSR) [1] - a recent

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

scheme to detect and avoid collaborative black hole attacks in MANETs - regarding network throughput rate and minimum packet loss percentage, when collaborative black hole nodes are present.

The performance of DSR protocol under black hole attack was analyzed and a solution called Enhanced Dynamic Source Routing (EDSR) protocol to detect it was suggested by Mohanapriya and Krishnamurthi [19]. This is a new ACK based detection technique capable of detecting when false data packets reached a destination thereby detecting black hole attacks. Experiments showed that the new protocol achieved routing security with 16% increase in packet delivery ratio and 31% reduction in packet loss rate compared to standard DSR under black hole attack. The new technique is light weight as it did not involve high computational complexity. It is scalable as it achieved better packet delivery ratio than standard DSR in a network of 200 nodes.

A mechanism to mitigate single and cooperative black hole attacks to discover a safe destination route by avoiding attacks was proposed by Mishra et al., [20]. An approach for better analysis and improved AODV security, a popular MANET routing protocol was proposed. The new scheme was AODV protocol based improved by deploying Advanced DRI table with additional check bit. Simulation on NS2 was done and the new scheme showed results demonstrating effectiveness of mechanism to detect and eliminate attack and maximize network performance by reducing packet dropping ratio.

Cooperative black hole attack, a new attack in adhoc networks was analyzed by Bhalaji et al., [21]. The suggested solution discovered a secure route amongst source and destination by recognizing and isolating cooperative black hole nodes. The new solution was evaluated through simulation and compared with existing solutions regarding throughput, packet delivery ratio and latency. Experiments were undertaken on network simulator-2 to validate the new research.

Simulating two routing protocols (AODV and DSR) under regular operation, single and cooperative black hole attack was done by Mohebi et al., [22]. The work was performed by simulator to show consequences of black hole attacks in MANETs by using graphs which collected data regarding several metrics. A common method to perform most MANET security research is to simulate and analyze routing protocols in various scenarios. The presented work is based on implementation and experiments in OPNET modeler version 14.5. Finally, results were computed/compared to locate which protocol is least affected by attacks.

Existing solutions were surveyed and state-of-the-art routing methods were discussed by Tseng et al., [23]. The authors classified proposals into single and collaborative black hole attacks and analyzed the solution categories through a comparison table. The authors are expected to furnish more research soon.

A counter calculation to distinguish malicious node in DSR protocol experiencing black hole attack was proposed by Bavarva and Modi [24]. Subsequently a change in packet delivery ratio (PDR) and average End-to-End delay were revealed through experiments.

Shinh and Singh [25] stated that routing attack in DSR protocol of MANET was black hole attack in which a malicious node presents itself as best short destination route. A strategy was described to detect and isolate multiple black hole attack in MANETs.

An algorithmic approach to analyze and improve security of AODV, a popular MANET routing protocols was proposed by Das et al., [26]. The work aimed to ensure security against black hole attacks. The new solution could detect and remove black hole node(s) in MANET at the beginning. The objective of the new work was a simulation study illustrating the effects of black hole attack on network performance.

3. METHODOLOGY

A new, secure DSR Routing protocol for MANETs is proposed based on trust and reputation to mitigate black hole attacks.

3.1 Dynamic Source Routing (DSR)

DSR is a reactive protocol and an example of an on-demand routing protocol based on source routing concept. It is meant for use in multi hop adhoc networks of mobile nodes. It allows a network to be self-organizing and self-configuring without any network infrastructure/administration. DSR routing protocol discovers routes and retains information regarding them from one node to other by using two mechanisms [27]: (i) Route discovery – locates route between source and destination and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(ii) Route maintenance –when a route fails, it invokes another destination route. DSR's advantage is source routing.

Route Discovery and Route Maintenance operate *on demand*. Unlike other protocols, DSR needs *no* periodic packets of *any kind* at *any level* within a network. For example, DSR does not resort to periodic routing advertisement, link status sensing, or neighbor detection packets. It also does not rely on these functions from any underlying network protocols. This total on-demand behavior and lack of periodic activity enables overhead packets caused by DSR to scale down to *zero*, when nodes are nearly stationary regarding each other and routes needed for current communication are already discovered. As nodes move more or as communication pattern changes, DSR routing packet overhead *automatically* scales to only track routes in use [28].

The DSR route request format is encoded as in table 1:

Table - 1 : Message FORMAT FOR Dsr Route Request (Rreq)

<table>
<tr><td colspan="2">Option Type</td><td colspan="2">Option Length</td><td colspan="2">Identification</td><td colspan="2">Trust Value</td></tr>
<tr><td colspan="8">Target Address</td></tr>
<tr><td>C</td><td>IN Index [1]</td><td>C</td><td>IN Index [2]</td><td>C</td><td>IN Index [3]</td><td>C</td><td>IN Index [4]</td></tr>
<tr><td>C</td><td>OUT Index [1]</td><td>C</td><td>OUT Index [2]</td><td>C</td><td>OUT Index [3]</td><td>C</td><td>OUT Index [4]</td></tr>
<tr><td colspan="8">Address [1]</td></tr>
<tr><td colspan="8">Address [2]</td></tr>
<tr><td colspan="8">Address [3]</td></tr>
<tr><td colspan="8">Address [4]</td></tr>
<tr><td>C</td><td>IN Index [5]</td><td>C</td><td>IN Index [6]</td><td>C</td><td>IN Index [7]</td><td>C</td><td>IN Index [8]</td></tr>
<tr><td>C</td><td>OUT Index [5]</td><td>C</td><td>OUT Index [6]</td><td>C</td><td>OUT Index [7]</td><td>C</td><td>OUT Index [8]</td></tr>
<tr><td colspan="8">Address [5]</td></tr>
</table>

Option Length - length of option is 8-bit unsigned integer in octets

Identification - A unique value is generated by the initiator of the route request.

C - Change Interface bit [1… n]

When data link layer detects a link disconnection in DSR, a ROUTE_ERROR packet is sent back to source. On receipt of ROUTE_ERROR packet, source node initiates another route discovery operation [29]. Additionally, routes containing broken link are removed from route caches of immediate nodes when ROUTE_ERROR packet is transmitted to source. Trust of node is very important in wireless networks. If a node/route has very low trust value, this route is dangerous. It also can have bad effect on network data packets: there are some nodes which are dropped.

Routing protocol uses path with larger trust value and less packet delay among multiple route options as two metrics unlike standard DSR protocol which uses minimum hop count alone. The idea is to maximize preemptive route creation by choosing a secure route. How well trust of a route is estimated plays a big role in this protocol's performance [30].The trust model uses DSR's inherent features to derive and compute trust levels in other nodes.

Every node executing a trust model, measures its immediate neighbours accuracy and authenticity by monitoring their participation in packet forwarding. The sending node verifies different fields of source route header in forwarded IP packet for modifications through integrity checks. If they succeed, it confirms that the node has behaved benevolently and so its direct trust counter is increased. But, if integrity check fails or if forwarding node fails to transmit packet at all, then its corresponding direct trust measure decreases [31].

Trust is measured using three scenarios listed in table 2.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table - 2 : Measuring Trust

Trust metric	Monitored behavior	Attack addressed
Data packets forwarded	Data message /packet forwarding	Black-hole, sinkhole, selective forwarding, denial of service, selfish behavior
Control packets forwarded	Control message forwarding	Control/routing message dropping
Routing protocol execution	Routing protocol specific actions (reaction to specific routing messages)	Misbehaviors related to specific routing protocol actions

A generalized approach is using the following equation for trust calculation [32].

$$T_i^{A,B} = \frac{a_i S_i^{A,B} - b_i F_i^{A,B}}{c_i S_i^{A,B} + d_i F_i^{A,B}} \quad (1)$$

where $T_i^{A,B}$ is node's A *Trust* value regarding node B, $S_i^{A,B}$ is number of successful type *i* events that A has measured for B, $F_i^{A,B}$ *i* is number of failed type *i* events that A measured for B and a_i, b_i, $c_i$and d_i, represent weight/significance of a successful *versus* weight/significance of failed events. Based on this equation, a trust value $T_i^{A,B}$ is calculated for every monitored behavior. These behavior-related trust values are multiplied by a weight factor (W_i) reflecting the importance in security hierarchy and then summed up to form overall node trustworthiness, as in following equation (2).

$$DT^{A,B} = \sum_{i=1}^{k} W_i * T_i^{A,B} \quad (2)$$

3.2 Proposed Trust Model

For wireless network with n nodes, a set of all nodes is denoted as $S=\{s_1,s_2,\ldots,s_n\}$. After deployment pairs of nodes $\{s_i,s_j\}\subseteq S$may interact directly with each other to perform a specific task that needs cooperation. Such interaction is considered successful by s_i if s_j cooperates in task performance. The history of observed outcome between s_i and s_j, from perspective s_i, is recorded at any time t as a tuple, $H_{s_{ij}}^t = (\mathrm{c}_{s_{ij}}^t, \mathrm{d}_{s_{ij}}^t)$ where value of $\mathrm{c}_{s_{ij}}^t$ is number of successful interaction (cooperation) of s_j with s_i, while $\mathrm{d}_{s_{ij}}^t$ is number of unsuccessful interactions.

Various distributions like beta, binomial, Poisson, Gaussian, etc. represent an agent's (node) reputation. Recently, beta distribution is employed in many works. In particular, it provided a thorough treatment of beta distribution and its usefulness in reputation systems. Beta distribution is used due to its simplicity, strong foundation on statistical theory and that its computation requires two shape parameters which make it quite applicable for memory constrained nodes and, is appropriate in representing binary events probability distribution. Beta probability density function $f(p|v,\omega)$ is expressed using gamma function Γ as in equation (3) [33]:

$$f(p \mid v,\omega) = \frac{\Gamma(v+\omega)}{\Gamma(v)\Gamma(\omega)} p^{v-1}(1-\mathrm{p})^{\omega-1}$$
$$0 \le p \le 1, v > 0, \omega > 0, \quad (3)$$

with restriction that probability variable $p \neq 0$ if $v < 1$, and $p \neq 1$ if $\omega < 1$.

Journal of Theoretical and Applied Information Technology
10th July 2015. Vol.77. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Consider interaction of two nodes s_i and s_j, from perspective of s_i there are two possible outcomes $O_{S_{ij}}=1$ for successful interaction and $O_{S_{ij}}=0$ for unsuccessful interaction. In this context $\mathrm{c}^t_{s_{ij}}$ and $\mathrm{d}^t_{s_{ij}}$,whichare defined previously also $O_{S_{ij}}=1$ $\mathrm{c}^t_{s_{ij}}$ mean that the outcome is observed $\bar{O}_{S_{ij}}$ $\mathrm{d}^t_{s_{ij}}$ times and is observed to occur times. The probability density function of observing outcome $O_{S_{ij}}=1$ in future can be expressed as a function of past observations by equation (5):

$$v=\mathrm{c}^t_{s_{ij}}+1 \text{ and } \omega=d^t_{s_{ij}}+1, \text{ where } \mathrm{c}^t_{s_{ij}},\mathrm{d}^t_{s_{ij}}\geq 0 \quad (5)$$

The expectation value for the beta distribution is defined as: $E(p)=v/(v+\omega)$, where p is probability variable.

Reputation of node s_j that is maintained at node s_i at any time t is defined as in equation (6):

$$R^t_{s_{ij}}=\frac{\Gamma(v+\omega)}{\Gamma(v)\Gamma(\omega)}p^v(1-p)^\omega \quad \text{where } 0\leq p\leq 1, v>0, \omega>0 \quad (6)$$

setting

$$v=\mathrm{c}^t_{s_{ij}}+1 \text{ and } \omega=d^t_{s_{ij}}+1, \text{ where } \mathrm{c}^t_{s_{ij}},\mathrm{d}^t_{s_{ij}}\geq 0$$

Given reputation, $R^t_{s_{ij}}$, between two nodes s_i and s_j, reputation q time later, $R^{(t+q)}_{s_{ij}}$, where $q>0$, is obtained by incorporating number of successful interactions $\mathrm{c}^{(t+q)-t}_{s_{ij}}$ and number of unsuccessful interactions $d^{(t+q)-t}_{s_{ij}}$ during period t to $t+q$ as in equation (7):

$$\mathrm{c}^{(t+q)}_{s_{ij}}=\mathrm{c}^t_{s_{ij}}+\mathrm{c}^{(t+q)-t}_{s_{ij}};\ \mathrm{d}^{(t+q)}_{s_{ij}}=d^t_{s_{ij}}+d^{(t+q)-t}_{s_{ij}}$$
$$\mathrm{R}^{(t+q)}_{s_{ij}}=Beta(\mathrm{c}^{t+q}_{s_{ij}}+1,\mathrm{d}^{t+q}_{s_{ij}}+1) \quad (7)$$

4. EXPERIMENTAL RESULTS

Experimental Setup

In this study, 80 number of nodes are used. The area considered is 4 sq. km with 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:

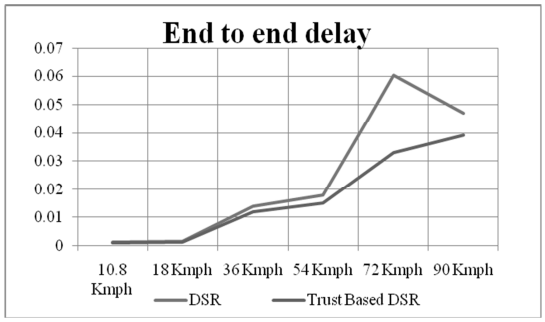

Figure - 1: End to End delay

The proposed trust based DSR reduced end to end delay by 57.9598% as highest value when compared with DSR in 72 kmph (Kilo Meter Per Hour) of node mobility. The proposed trust based DSR reduced end to end delay by 13.4591% as least value when compared with DSR in 36 kmph of node mobility. Averagely trust based DSR reduced by 32.5123% of end to end delay when compared with DSR with 10% of malicious nodes in network.

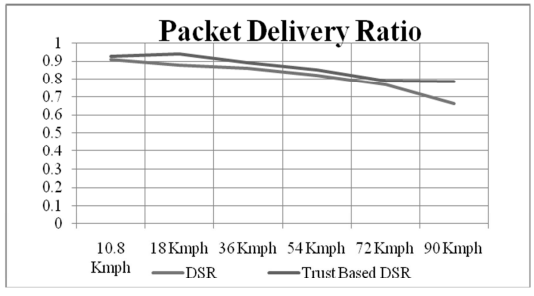

Figure - 2: Packet delivery ratio

Journal of Theoretical and Applied Information Technology
10th July 2015. Vol.77. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The proposed trust based DSR improved packet delivery ratio by 17.1413 % as highest value when compared with DSR in 90 kmph of node mobility. The proposed trust based DSR improved packet delivery ratio by 1.7435 % as least value when compared with DSR in 10.8 kmph of node mobility. Averagely trust based DSR improved by 5.6864 % of packet delivery ratio when compared with DSR with 10% of malicious nodes in network.

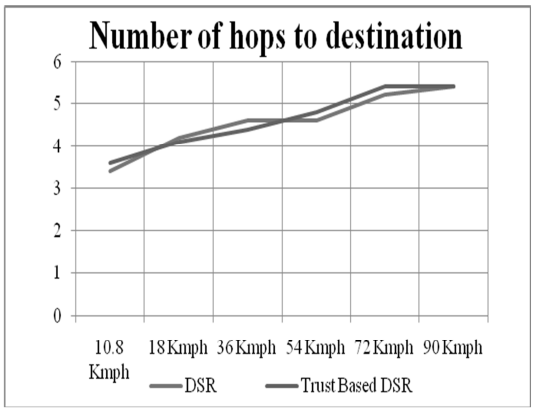

Figure – 3 : Number of hops to destination

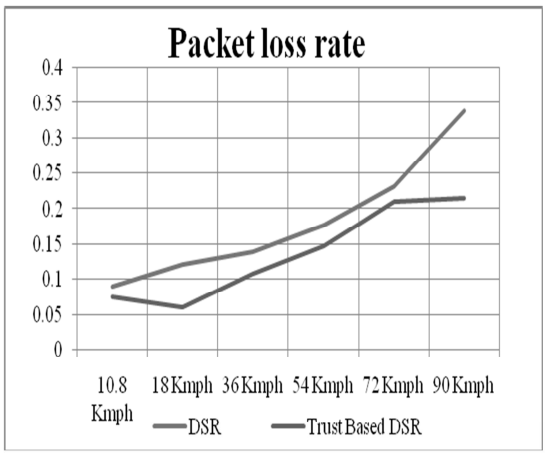

Figure -4 : Packet loss rate

The proposed trust based DSR reduced Packet loss rate by 68.1391% as highest value when compared with DSR in 18 kmph of node mobility. The proposed trust based DSR reduced Packet loss rate by 10.2645% as least value when compared with DSR in 72 kmph of node mobility. Averagely trust based DSR reduced by 29.9875% of Packet loss rate when compared with DSR with 10% of malicious nodes in network.

The experimental results for 20% of malicious nodes are shown in figures (5 to 8) as follows:

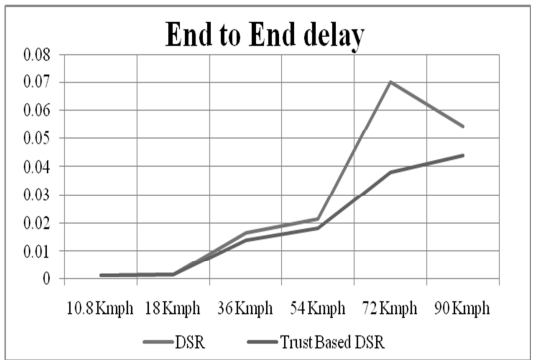

Figure - 5 : End to End delay

The proposed trust based DSR reduced End to End delay by 58.9322% as highest value when compared with DSR in 72 kmph of node mobility. The proposed trust based DSR reduced End to End delay by 11.7033% as least value when compared with DSR in 10.8 kmph of node mobility. Averagely trust based DSR reduced by 34.89% of End to End delay when compared with DSR with 20% of malicious nodes in network.

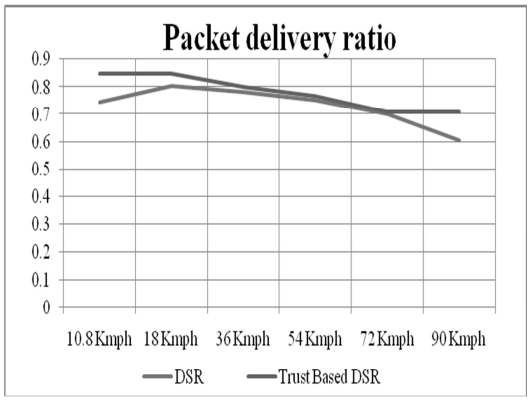

Figure - 6 : Packet Delivery Ratio

oved Packet Delivery Ratio by 16.2055% as highest value when compared with DSR in 90 kmph of node mobility. The proposed trust based DSR improved Packet Delivery Ratio by 1.5609% as

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

least value when compared with DSR in 72 kmph of node mobility. Averagely trust based DSR improved by 6.5591% of Packet Delivery Ratio when compared with DSR with 20% of malicious nodes in network.

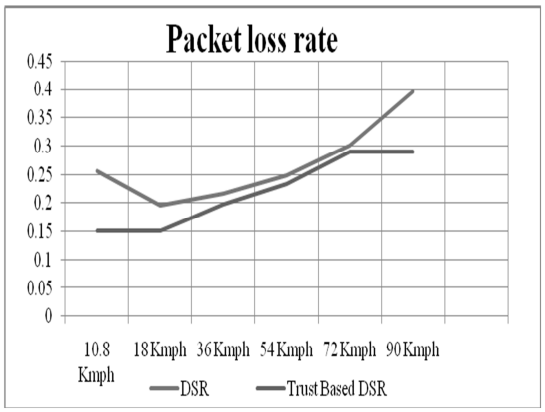

Figure - 8 : Packet loss rate

The proposed trust based DSR reduced Packet loss rate by 50.8707% as highest value when compared with DSR in 10.8 kmph of node mobility. The proposed trust based DSR reduced Packet loss rate by 3.725% as least value when compared with DSR in 72 kmph of node mobility. Averagely trust based DSR reduced by 20.3814% of Packet loss rate when compared with DSR with 20% of malicious nodes in network.

5. CONCLUSION

As MANET is quickly spreading due to its capability to form temporary network without any established infrastructure / centralized administration, security challenges are a primary concern to ensure secure communication. This study proposed trust based DSR. Experiments are undertaken with 10% and 20% malicious nodes respectively. Trust based DSR improved packet delivery ratio in both experiments and greatly reduced end to end delay and packet loss rate. Number of hops to destination is more or less same as with DSR. Results demonstrated that the new method outperformed traditional DSR.

REFERENCES:

[1]. Sumyla, D. (2006). "Mobile Ad-hoc Networks (MANETS)", Technical Report.

[2]. Chlamtac, I., Conti, M., & Liu, J. J. N. (2003), "Mobile ad hoc networking: imperatives and challenges", Ad Hoc Networks, 1(1), pp. 13-64.

[3]. Raghavendran, C. V., Satish, G. N., & Varma, P. S. (2012), "Intelligent Routing Techniques for Mobile Ad hoc Networks using Swarm Intelligence", International Journal of Intelligent Systems and Applications (IJISA), 5(1), 81.

[4]. Gomathi, S., Poonkuzhali, R., & Duraiswamy, K. (2008), "Routing protocols for mobile ad-hoc networks performance enhancement", Journal of Computer Applications, 1(4), 38.

[5]. Rath, B. (2009), "Implementing and Comparing DSR and DSDV Routing Protocols for Mobile Ad Hoc Networking", (Doctoral dissertation, National Institute of Technology Rourkela).

[6]. Rao, D. J., Sreenu, K., & Kalpana, P. (2012). "A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks", International Journal of Advanced Research in Computer and Communication Engineering, 1(8), pp. 2319-5940.

[7]. Ullah, I., & Rehman, S. U. (2010), "Analysis of Black Hole attack on MANETs Using different MANET routing protocols", *School of Computing Blekinge Institute of Technology, Sweden*.

[8]. Shanmuganathan, V., & Anand, T. "A Survey on Gray Hole Attack in MANET", *International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN*-2250-3501.

[9]. 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), pp. 12-18.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[10]. Jawandhiya, P. M., Ghonge, M. M., Ali, M. S., & Deshpande, J. S. (2010), "A survey of mobile ad hoc network attacks", *International Journal of Engineering Science and Technology*, *2*(9), pp. 4063-4071.

[11]. Srinivasan, A., Teitelbaum, J., Wu, J., Cardei, M., & Liang, H. (2009), "Reputation-and-Trust-Based Systems for Ad Hoc Networks. Algorithms and protocols for wireless and mobile ad hoc networks", 375.

[12]. Sardar, M., & Majumder, K. (2013), "A survey on trust based secure routing in MANET", Computer Science.

[13]. Sekhar, J. C., & Prasad, R. S. (2014), "Design of novel security architecture for MANET for trusting and authentication", Journal of Theoretical & Applied Information Technology, 61(2).

[14]. Soni, H., & Verma, P. (2013), "A Survey of Performance based Secure Routing Protocols in MANET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2(1), 145.

[15]. Tsou, P. C., Chang, J. M., Lin, Y. H., Chao, H. C., & Chen, J. L. (2011, February), "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs", In Advanced Communication Technology (ICACT), 2011 13th International Conference on (pp. 755-760). IEEE.

[16]. Cai, J., Yi, P., Chen, J., Wang, Z., & Liu, N. (2010, April), "An adaptive approach to detecting black and gray hole attacks in ad hoc network", In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on (pp. 775-780). IEEE.

[17]. Patil, P. N., & Bhole, A. T. (2013, July), "Black hole attack prevention in mobile Ad Hoc networks using route caching", In Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on (pp. 1-6). IEEE.

[18]. Woungang, I., Dhurandher, S. K., Peddi, R. D., & Traore, I. (2013), "Mitigating collaborative blackhole attacks on DSR-Based mobile ad hoc networks", In Foundations and Practice of Security (pp. 308-323). Springer Berlin Heidelberg.

[19]. Mohanapriya, M., & Krishnamurthi, I. (2013), "A Light-Weight and Scalable Solution for Secure Routing in DSR MANET for Black Hole Attack", Ad-hoc & sensor wireless networks, 17(1-2), pp. 33-52.

[20]. Mishra, A., Jaiswal, R., & Sharma, S. (2013, February), "A novel approach for detecting and eliminating cooperative black hole attack using advanced dri table in ad hoc network", In Advance Computing Conference (IACC), 2013 IEEE 3rd International (pp. 499-504). IEEE.

[21]. Bhalaji, N., Kanakeri, A. V., Chaitanya, K. P., & Shanmugam, A. (2010), "Trust based strategy to resist collaborative blackhole attack in MANET", In Information Processing and Management (pp. 468-474). Springer Berlin Heidelberg.

[22]. Mohebi, A., Kamal, E., & Scott, S. (2013), "Simulation and Analysis of AODV and DSR Routing Protocol under Black Hole Attack", International Journal of Modern Education and Computer Science (IJMECS), 5(10), 19.

[23]. Tseng, F. H., Chou, L. D., & Chao, H. C. (2011), "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences, 1(1), pp. 1-16.

[24]. Bavarva, P., & Modi, P. (2014), "Preventing DSR routing protocol against Black Hole using Counting Method", International Journal of Advance Engineer ing and Research Development (IJAERD), 1(5).

[25]. Shinh, B., & Singh, M. (2014), "Detection and Isolation of Multiple Black Hole Attack Using Modified DSR", International Journal of Emerging Trends in Science and Technology, 1(04).

[26]. Das, R., Purkayastha, B. S., & Das, P. (2012), "Security Measures for Black Hole

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Attack in MANET: An Approach", arXiv preprint arXiv:1206.3764.

[27]. Singh, R., Singh, D. K., & Kumar, L. (2011), "Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks", *Int. J. Advanced Networking and Applications*, *2*(04), pp. 732-737.

[28]. Maltz, D. B. J. D. A., & Broch, J. (2001), "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks", *Computer Science Department Carnegie Mellon University Pittsburgh, PA*, 15213-3891.

[29]. Wang, C., Yang, X., & Gao, Y. (2005), "A routing protocol based on trust for MANETs", In *Grid and Cooperative Computing-GCC 2005* (pp. 959-964). Springer Berlin Heidelberg.

[30]. Lavanya, G., & Jeyakumar, A. E. (2011), "An enhanced secured dynamic source routing protocol for MANETS", *International Journal of Soft Computing and Engineering*, *10*, pp. 135-140.

[31]. Samundiswary, P., & Dananjayan, P. (2010, February), "Secured dynamic source routing protocol for mobile sensor networks", In *Proc of the 12th International Conference on Networking, VLSI and Signal Processing*.

[32]. Zahariadis, T., Leligou, H. C., Trakadas, P., & Voliotis, S. (2010), "Trust management in wireless sensor networks", *European Transactions on Telecommunications*, *21*(4), pp. 386-395.

[33]. Crosby, G. V., & Pissinou, N. (2007, January), "Cluster-based reputation and trust for wireless sensor networks", In *Consumer Communications and Networking Conference*.