International Journal of Future Generation Communication and Networking
Vol. 8, No. 1 (2015), pp. 137-148
http://dx.doi.org/10.14257/ijfgcn.2015.8.1.15

Improved Trust Based Routing Mechanism in DSR Routing Protocol in MANETs

Ankita Sahu[1] and Vikas Sejwar[2]

[1]*Department of CSE/IT, Madhav Institute of Technology and Science Gwalior MP India,*

[2]*Assistant Professor,Department of CSE/IT, Madhav Institute of Technology and Science Gwalior MP India,*

[1]*ankitasahu63@gmail.com,* [2]*vikassejwar@gmail.com*

Abstract

Mobile Ad hoc Network (MANET) is a self organizing wireless network for mobile devices. They do not need any fixed infrastructure to be configured which makes it more suitable to be used in environments that require on-the-fly setup. The present work discusses the challenging issues in MANET routing security. It presents improved DSR, a trust-based scheme for securing DSR routing protocol in MANET using the friendship mechanism and gateway. The path which is most optimum is chosen as the final route from source to destination. The gateway nodes should not be malicious .The nodes can evaluate the routing paths according to some selected features (such as node reputation and identity information) before forwarding the data through these routes. It is implemented in our scheme, simulation (using NS2). This scheme provides a robust environment where MANET nodes can trust each other in a secure community. Experimental results show that our gateway based DSR improves network performance to much extent.

Keywords: *Mobile ad hoc network, security, Trust feature, DSR Protocol, RREP, RREQ.*

1. Introduction

Infrastructure networks are not suitable in environments where limited resources devices are connected through weak wireless links. In this case, the network should be able to setup on-the-fly without the aid of any administrator or manager. MANET is one solution for such environments. It is a self-organizing and self-configuring network. It is established on a temporary basis and nodes can join or leave the network at any time. For example, new nodes can quickly join or leave the network in a conference room, battlefield or fire operation area. The lack of infrastructure and the mobility features of MANET make the routing security process a difficult task. MANET is vulnerable to many routing attacks such as redirection attack where a malicious node sends forged Rrep (Route Replay) messages with high destination sequence numbers [1].

The source node chooses the routes with the highest destination sequence numbers and discards the other routes. All data sent by the source node will be directed through these routes towards the malicious node which in turn drops this data instead of forwarding it [1]. Another famous routing attack are rushing attacks which usually happen in the reactive routing protocols where each node considers just the first route discovery packet that it receives and discards the others [2]. In this attack, malicious nodes rush route requests towards the destination which will consider these requests and ignore the others. The destination node then replies to these requests. As a result, all source and destination traffic will go through the malicious nodes [2].

ISSN: 2233-7857 IJFGCN

Many researchers have proposed different methods to secure the routing protocols. In this research, we focus on securing DSR routing protocol. SDSR protocol has been proposed to secure DSR [3], in which both AODV messages (Rreq, Rrep) and the mutable information (hop count, hash value) is included in the protection mechanism. Each node signs Rreq and Rrep message after reducing the hop count and the hash value fields, in which these fields are changed in every hop. The signing process is accomplished by using asymmetric cryptography. SDSR can defend against black hole attack [4]. However, it cannot defend against worm-hole attack [5], hop-count altering attack and routing messages dropping attack. In this paper, friendship based DSR routing protocol has been implemented in a simulation mode (using NS2) using gateway. Some trust features are identified to evaluate the node friendship in the network. A friendship mechanism algorithm is constructed to secure DSR routing protocol.

The paper is organized as follows: Section 2 describes some preliminaries about MANET and trust concept. Section 3 presents conventional DSR scheme. Our scheme is explained in Section 4.The performance evaluation of our proposed scheme for simulation and real test-bed scenario are presented in Section 5. Section 6 describes the results of simulation. The paper is concluded with suggestions for future work in Section 7.

2. Trust based Security in MANET

The traditional cryptography schemes that provide authentication and data privacy do not detect when an internal node provides false routing information, or where a node does not cooperate with the other nodes to save its resources.

There should be another layer of security that detects such misbehavior. This layer is based on trust concept. This concept was first proposed in the early 80's. It is based on the way that human beings trust each other. When a person wants to verify another person, he usually asks his friends about this person. He also asks this person to provide him with the list of reference people who will be asked if he is to be trusted. In the same way, step, S requests recommendations from the list of trusted entities (friends). This request implies a question to each entity in the list about the identity of D. Each entity answers yes (trusted) or no (un-trusted). Any entity that does not find D in its friends list forwards the request to its trusted entities list (Recommendation list). If any entity of the friends list or the recommendation list knows D and trusts him, information about D is sent back to S. In the next step, node S will ask D about the references, i.e. other entities with which he has communicated before. When S receives D references, he asks his friends list if they know these references and trusts them. S also may ask the references for references. In references also proposed to use the trust concept to evaluate the nodes in MANET.

NEIGHBOUR_ID	TRUST VALUE

Figure 1. Neighbour Table

Destination IP	Destination sequence no.	Hop count	Next hop	..	..	Route trust

Fig 2. Modified Extended Routing Table

2.1. DSR Protocol

The Dynamic Source Routing (DSR) protocol is a reactive routing protocol. As the name suggests it makes use of the strict source routing feature of the Internet Protocol. All data packets that are sent using the DSR protocol contain the complete list of nodes that the packet has to traverse. During discovery of route , the source node broadcasts a ROUTE REQUEST packet with a unique identification number. The ROUTE REQUEST packet has the address of the target node to which a route is desired.

All those nodes that have no information regarding the target node, or have not previously seen the same RREQ packet, append their IP addresses to the RREQ packet and re-broadcast it. In order to control the spread of the ROUTE REQUEST packets, the broadcast is done in a non-propagating manner with the IP TTL field being incremented in each route discovery.

The former stores complete paths to a particular destination, while the latter only caches information related to individual links. The advantage of the LINK CACHE scheme is that it allows alternate paths to a destination even when some of the intermediate links have failed.

Each node either forwarding or overhearing data and control packets, adds all useful information to its respective route cache. This information is used to limit the spread of control packets in subsequent route discoveries.

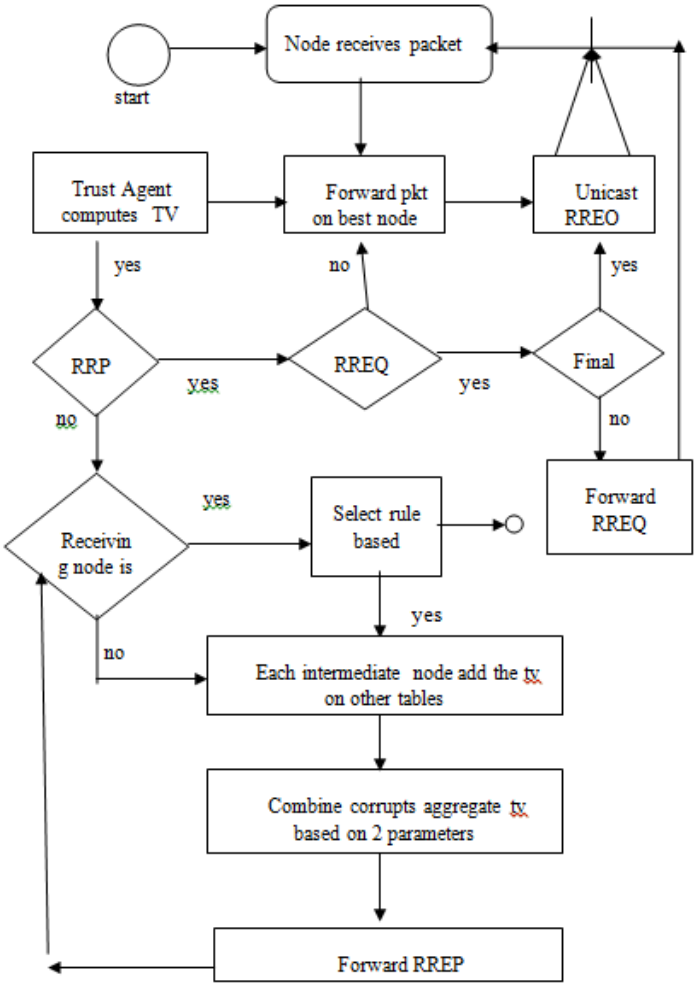

Figure 3. Process Flow for Route Selection

3. Feature Selection in Trust based Security in MANET

A good features selection scheme plays an important role in creating a trust-based MANET community. Features actually represent the characteristics or evidence properties of each node in the network. We had made a set of comparative studies on several features selection schemes in our previous work. In general, feature based schemes can be divided into 2 categories including performance metrics evaluation and quantitative trust value. In the category of performance metrics evaluation, the efficiency of selected features are evaluated by using certain metrics such as routing traffic, route discovery time, routing overhead and number of data packets delivery. For instance, each feature contains its own corresponding attribute number that will be presented during packet forwarding process . When a source node wants to forward a packet to its destination, it will ask its neighboring nodes to present their feature's attribute number for checking. If the neighboring nodes manage to present an attribute number that fulfills the source node's requirement, the attribute number will be embedded in the packet format and the node is granted to forward the packet to other neighboring nodes before reaching the required destination.

The effectiveness of packet forwarding process based on selected features are measured using performance metrics such as Encryption / Key, Hardware Configuration, Battery Power, Credit History/ACK, Exposure, Organization Hierarchy, Identity, and Location. On the other hand, the quantitative trust value category represents the method of evaluating trust features by using certain mathematical functions or equations. Each feature has its own trust value metric that can be assigned based on one's judgment for a specific application. At present, there is no standard to determine value metrics. The values are determined based on intuitive decisions. The features' trust value metrics are computed in a formulated equation and the output will be used to determine whether a node can be trusted or vice versa. According to recent research , there are eight features which can be considered for performance metrics evaluation and ten features for quantitative trust value. Three features that are not very useful for both categories are battery power, credit history or acknowledgement and identity which were proposed in .The other frequently used potential selected feature is encryption or key type which falls under the performance metrics evaluation category. The remaining expected suitable features are trust value metric, packet precision and blacklist.

In this paper, we have considered 3 features to represent each node in our MANET environment which includes trust value metric, packet precision and blacklists. As aforementioned in, the selection of these features is based on the justification that they have been frequently used in the previous six research works . However, these features are subject to change after an emulation process has been carried out, which may give results on the suitability of the features used. The remaining unselected features are not discarded but are reserved for later deployment, for example, in case the current selected features are found to have weaknesses.

4. Proposed Scheme

In this section, we present our friendship-based framework proposed to secure DSR (Fig. 1). Two algorithms are used here forward and reverse routes respectively in DSR protocol.

Steps of our Algorithm :

Step 1:

S is the source node. D is the intended destination

Step 2:

S sends the data packets to neighbors and update its routing table as per the forwarding packets number

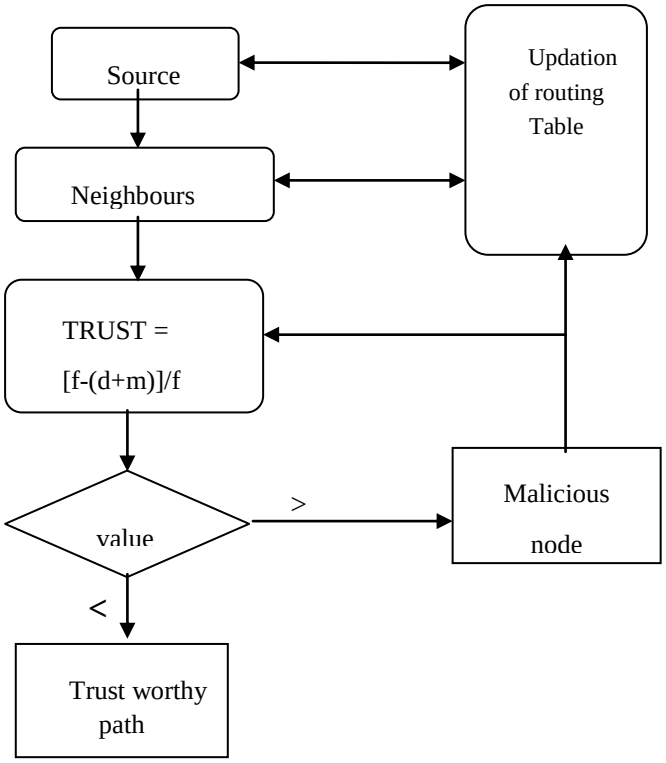

Fig 4: Proposed Algorithm Flowchart

Step 3:
The neighbors also forward the routing packets further and the trust value is calculated as per the following formula of step 4

Step 4: Trust parameters
f= number of packets forwarded
d=number of packets dropped
m=number of packets misrouted

4.1**:** Collect data for f,d,m.
4.2: Calculate total number of packets which were dropped or misrouted i.e (d+m)
4.3:Calculate total number of packets which were successfully reached to the destination i.e (f-{d+m})
4.4: Calculate direct trust by using formula

Trust (t)= [f-(d+m)]/ f ……(1)

Step5:

If the value of the calculated trust exceeds the obtained value then it does not forward it to the next nodes and considers it as malicious. So the path becomes malicious gateway path. All neighbors are informed not to forward data packets via that route

Step 6:

If the obtained value is less than the threshold then the packets are forwarded and that gateway or path is considered as path of maximum trust.

Step 7:

In case when maximum values are trust values then the obtained maximum valued data packets are forwarded first and considered as path or gateways of that route.

We assume that each node has identity information that cannot be forged by malicious nodes. This Identity information can be some type of smart card provided in the initialization phase. For simplicity, we use IP and MAC addresses. The friends list is created in the initialization phase and distributed (offline) to the devices.

5. Simulation and Results

Nasty nodes create the following types of attacks against data and control packets:

1. Modification Attack. These attacks are carried out by adding, altering or deleting IP addresses from the ROUTE REQUEST, ROUTE REPLY, ROUTE ERROR and Data packets that pass through the malicious nodes.
2. Black Hole Attack. In this attack the malicious node drops all packets, which it is supposed to forward.
3. Grey Hole Attack. Here the malicious node selectively dumps data and control packets at random intervals. All malicious nodes work in a non-colluding manner. Each malicious node sporadically alters its attack profile by randomly switching between the three types of attacks.

The matrices used include:

* *Packet Drop*: It is a kind of denial of service attack in the packets i.e. the packets that were dumped by malicious nodes without any notification.

* *Packet delivery ratio (PDR):* The PDR in this simulation is defined as the ratio between the number of packets sent by constant bit rate sources and the number of received packets by the CBR sink at destination. It describes percentage of the packets which reach the destination.

$$PDR = \sum CRB\ PKtRevd\ / \sum CRB\ PKtSent$$

* *Packet forwarding*: It is the defined as the forwarding or direction of the packet traffic to the further nodes or neighbours to reach the destination

* *Packet Sent:* This is the correct forwarding of the packets to the group of nodes (multicast and broadcast) between the control packets and the data packets received during the simulation time.

* *Packet Receive*: It is the fraction of packets that were obtained by nodes after the multicast or broadcast.

The results are shown as:

The results are shown as:

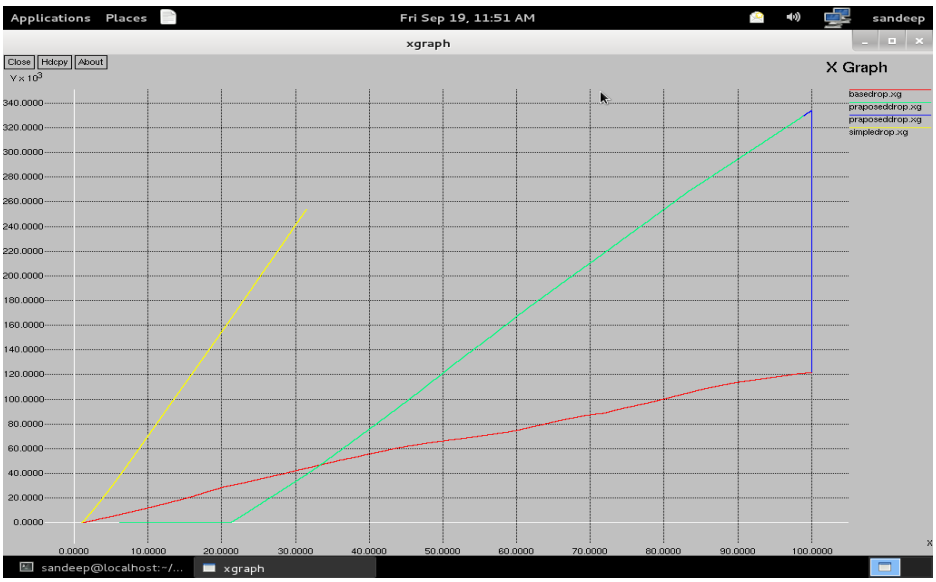

Figure 5. Packet Drop

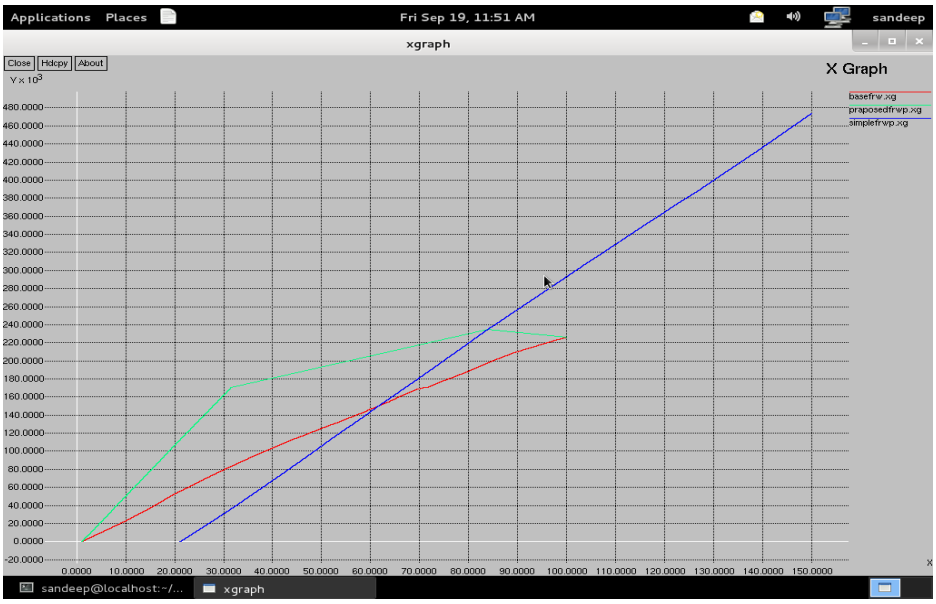

Figure 6. Packet Forward

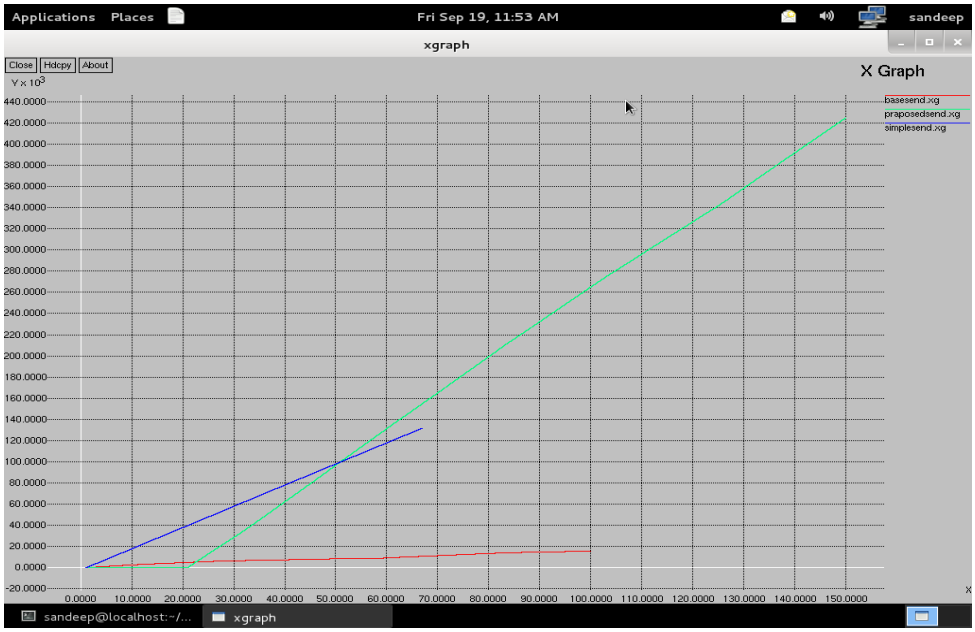

Figure 7. Packet Send

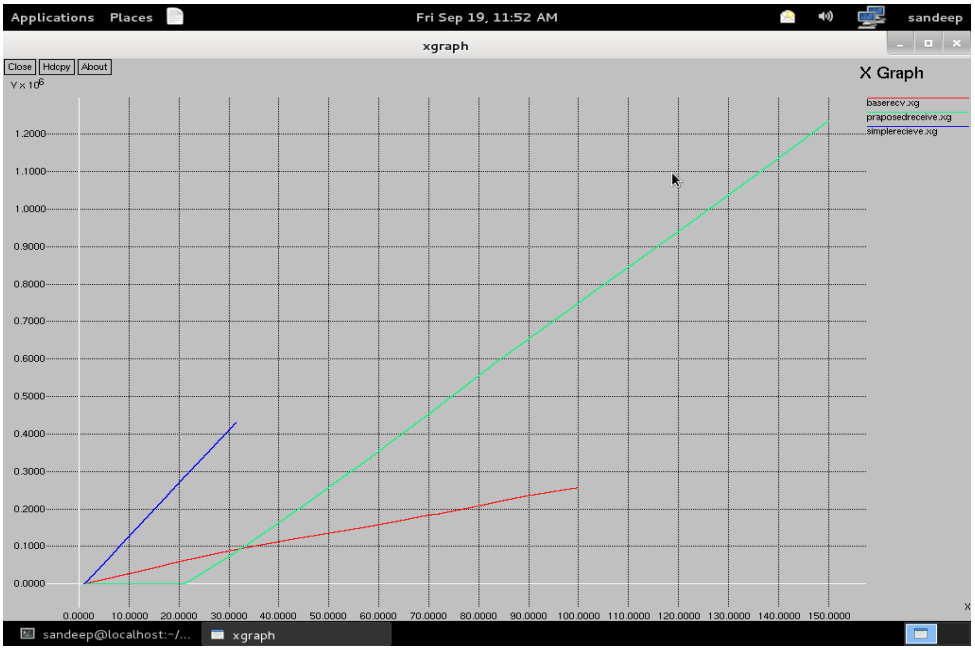

Fig 8: Packet Receive

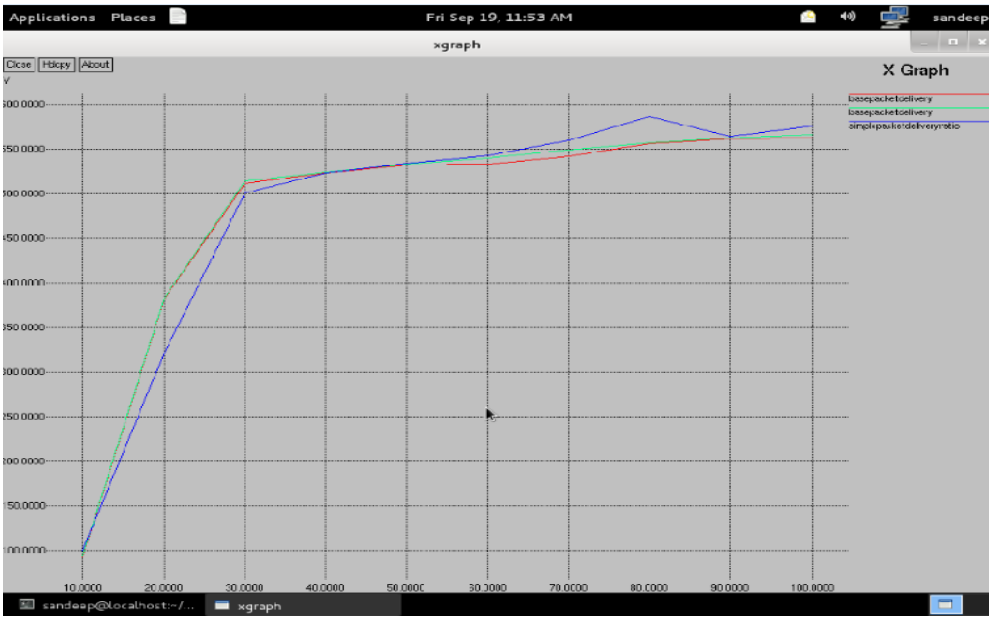

Figure 9. PDR (Packet Delivery Ratio)

Table 1. Simulation Parameter Value

Number of nodes	25
Simulation Time	Up to 5 minutes
Map size	Order of 1000
Mobility model	Random way point
Traffic type	Static
Packet size	Same in all cases
Connection Range(Nominal Radio range)	Average
Pause time	10 ms

6. Conclusion

In this paper, the proposed approach is the extension of existing DSR routing protocol for creating secure route for communication. Proposed modifications are in acceptable limit. With this minimum overhead, we can easily eliminate the malicious node as well as we can establish a best trusted route between source and destination. Also it creates a secure communication in this environment without any internal attackers. Using simulation results, the performance of this novel protocol is justified. In the future, it will be incorporate with other MANET routing protocols.

Ad-hoc networks are frequently targeted by participating malicious nodes to sabotage the network. A common mechanism to protect these networks is through the use of encryption and hashing mechanisms. However, the implementation of these mechanisms generally accompanies superfluous requirements, which are considered restrictive for impromptu environments. In order to maintain the makeshift nature of ad hoc networks, we have used an unusual approach of enforcing trust in the network. We have moved from the common mechanism of achieving trust in the network via security to enforcing dependability through collaboration. Each node in the network monitors its surrounding neighbours and maintains a direct trust value for them. These trust values are then used to make appropriate routing decisions both during the initiation phase as well as the forwarding phase. Nodes initiating a data connection create trustworthy paths through the network using their readily available direct trust information. This mechanism is then reinforced at the transitional stage through the use of Trust Gateways, where forwarding nodes perform trust based node filtering. This double trust corroboration scheme ensures that data is propagated on dependable routes in the network instead of standard shortest paths. Through extensive simulations we have found that the throughput of our proposed protocol remains notably higher than that of the standard DSR protocol in the presence of malicious nodes.

References

[1] C. S. R. Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Second Edition, Low price Edition, Pearson Education, **(2007)**.

[2] N. Tantubay, D. R. Gautam and M. K. Dhariwal, "A Review of Power Conservation in Wireless Mobile Adhoc Network (MANET)", IJCSI, vol. 8, no 1, **(2011)**.

[3] P. Nand and S. C. Sharma, "Performance study of Broadcast based Mobile Ad hoc Routing Protocols AODV, DSR and DYMO", International Journal of Security and Its Applications , vol. 5, no. 1, **(2011)**.

[4] I. G. Shayeb, A. R. H. Hussein and A .B. Nasoura, "A Survey of Clustering Schemes for Mobile Ad-Hoc Network (MANET)", American Journal of Scientific Research, **(2011)**, pp. 135-151.

[5] K. Erciyes, O. Dagdeviren, D. Cokuslu and D. Ozsoyellery, "Graph theoretic clustering algorithms in mobile ad hoc networks and wireless sensor networks", Applied and Computational Mathematics, vol. 6, no. 2, **(2007)**, pp. 162-180.

[6] G. Kumar, K. K. Tripathi and N. Tyag, "Research Survey of Load Balancing Clusters in Wireless Ad hoc Network", International Journal of Electronics Engineering, **(2011)**, pp. 305-307.

[7] J. Kong, H. Luo, K. Xu, D.L. Gu, M. Gerla, S. Lu, "Adaptive security for multilevel ad hoc networks", **(2002)**.

[8] N. S. Yadav and R. P. Yadav, "Performance Comparison and Analysis of Table- Driven and On-Demand Routing Protocols for Mobile Ad-hoc Networks", International Journal of Information Technology, vol. 4, no. 2, **(2007)**, pp 101-109.

[9] S. Chinara and S. K. Rath, "A Survey on One-Hop Clustering Algorithms in Mobile Ad Hoc Networks", Journal of Network and Systems Management archive, vol. 17, no. 1-2, **(2009)**, pp. 183-207.

[10] J. Zhang, "A Survey on Trust Management for VANETs", International Conference on Advanced Information Networking and Applications, **(2011)**, pp. 105-112.

[11] J. Duan, Y. Qin, S. Zhang, T. Zheng and H. Zhang, "Issues of Trust Management for Mobile Wireless Sensor Networks", 7th International Conference on Wireless Communications, Networking and Mobile Computing, **(2011)**, pp. 1-4.

[12] P. Nand and S. C. Sharma, "Performance study of Broadcast based Mobile Ad hoc Routing Protocols AODV, DSR and DYMO", International Journal of Security and Its Applications , vol. 5, no. 1, **(2011)**.

[13] J. H. Cho, A. Swami and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, **(2011)**, pp. 562-583.

[14] S. Mishra, A. X. Das and A. K.Jaisawal, "Effect of Mobility and Different Data Traffic in Wireless Ad-hoc Network through QualNet", International Journal of Engineering and Advanced Technology, vol. 2, no.5, **(2013)**.

Authors

Ankita Sahu, is a final year M.Tech student of Computer Science and Engineering Department at Madhav Institute of Technology & Science,Gwalior,India. Her areas of interest are Network security in Ad hoc Networks. She can be reached at ankitasahu63@gmail.com.

Vikas Sejwar is presently Assistant Professor in computer science and engineering department at Madhav Institute of Technology & Science, Gwalior, India. He has got M.Tech degree from SOIT, RGPV, Bhopal in 2008. He has got B.E. degree from MITS, Gwalior in 2006. His research area includes Mobile Adhoc Network and Computer graphics.