Asian Journal of Information Technology 7 (8): 350-355, 2008
ISSN: 1682-3915

Improved DSR Protocol for the Malicious Nodes in Mobile Adhoc Networks

[1]N. Bhalaji and [2]A. Shanmugam
[1]University of Hindustan, Chennai, India
[2]Bannari Amman Institute of Technology, Erode, India

Abstract: In a Mobile Adhoc Network (MANET) is a special type of mobile wireless network, where a collection of mobile network without any aid of an established infrastructure. Security issues put challenges in MANET routing protocol design. This study focuses on the simulation study for security of routing protocol for MANET and particularly on the improvement of Dynamic Source Routing protocol (DSR) security. In this conceptual study, we propose an idea to include Acknowledgement monitor as a component of existing extended DSR protocol. Different simulations are performed on the NS-2 network simulator to evaluate the performance impacts of applying above concepts to DSR protocol and results are analyzed.

Key words: Malicious nodes, DSR, grudger, adhoc network

INTRODUCTION

The advancement in telecommunication Technologies has brought up several Communication alternatives that can be selected from. One of the most popular technologies that currently been used widespread is wireless network. Wireless network is a telecommunication network whose interconnections between nodes are implemented without the use of wires. This study will focus on discussing the security vulnerabilities in the wireless network that fill in the category of networks that donot have fixed infrastructure or known as mobile adhoc network (MANET). A MANET consists of mobile nodes, which are Free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices and there may be multiple hosts per router (Johnson *et al*., 2001). An adhoc network doesn't have centralized Controller such as router to determine the route of the paths. Thus, each node in an adhoc Network has to rely on each other in order to forward packets. Every node can operate both as a host and a router at a time and there's a need to Use a specific cooperation mechanism to forward Packet from hop to hop before it reaches a required destination by using routing protocol. Examples of available routing protocols for adhoc network are Adhoc On-demand Distance Vector (AODV), Zone Routing Protocol (ZRP), Destination Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR).

The DSR protocol: Dynamic source routing is a protocol developed for routing in mobile adhoc networks and was proposed for MANET by Johnson *et al*. (2001). In a nutshell, it works as follows: Nodes send out a ROUTE REQUEST message, all nodes that receive this message put themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or are gratuitous. After receiving one or several routes, the source selects the best (by default the shortest), stores it and sends messages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. When a ROUTE REPLY arrives very quickly after a ROUTE REQUEST has been sent out this is an indication of a short path, since the nodes are required to wait for a time corresponding to the length of the route they can advertise, before sending it. This is done, in order to avoid a storm of replies. In case of a link failure, the node that cannot forward the packet to the next node sends an error message towards the source. Routes that contain a failed link can be `salvaged' by taking an alternate partial route that does not contain the bad link.

Active attacks: Active attacks could severely harm a network system because the type of attacks that are

Corresponding Author: N. Bhalaji, Department of Information Technology, University of Hindustan, India

launched can generate message falsification, chaos routing table and hardware failure. There are 4 categories of active attacks as follows:

Masquerading: Impersonation of one node (malicious node) to become another node that it's actually not. The malicious node can perform the same function as the actual node does but in illegal purposes. For example, a malicious node could forge legitimate routing message to be sent to wrong destination that make routing table inconsistent.

Replay: An attacker gains unauthorized information in a passive manner and use it to broadcast false instruction that could cause problems such as incorrect routing path selection and forwarding packet to illegitimate receiver.

Modification: Alteration of the content of an original message or fields of routing message to create unauthorized access. Modification can also be in the form of delaying and reordering the message.

Denial of Service (DoS): The main purpose of this attack is to degrade the performance of a network system. Intruders may inject thousands of false routing messages into the system to purposely push CPU to process them. As a result, the network resource and time is wasted for processing those bogus messages.

Passive attacks: Passive attacks as opposed with active attacks are launched by intruders to merely analyze certain information that is being transmitted. There are 2 types of passive attacks are discussed:

Release of message contents: Intruders try to learn the content of certain confidential information that they can manipulate to identify an identity of a node.

Traffic analysis: This type of attack is launched by intruders as an alternative to learn the information that is well protected by encryption algorithm. By observing the Pattern of the traffic, they might gain information like the location and the identity of the communicating nodes.

Some of the related works and new secure routing schemas that are being developed are analyzed in the section (Giuli *et al*., 2000). In this proposed scheme using extended DSR, the problem of forwarding defection is taken up for simulation and performance analysis as it is the simplest of all problems to deal with.

THE GRUDGER PROTOCOL

It is an application from a biological example proposed by Dawkins (1976), which explains the survival chances of birds grooming parasites off each others head. Dawkins introduces 3 categories of the birds namely:

- Suckers, which are good natured, helpful and favor others by grooming parasites off others head.
- Cheats, which get help from others but fail to return the favor.
- Grudger who starts out being helpful to every bird, but bears a grudge against those birds that don't return the favor and subsequently no longer help them.

In an adhoc network, grudger nodes are introduced, which employ a neighborhood watch by keeping track of what is happening to other nodes in the neighborhood, before they have a bad experience themselves. They also share information of experienced malicious behavior with friends and learn from them. The protocol consists of the following components:

Monitor: It registers deviation of normal behavior and manages them in the watch table. On detection of bad behavior, an alarm is sent to the reputation system and trust manager.

Reputation system: It manages a table consisting of entries for nodes and their rating. Local rating lists or black lists are maintained with friends and potentially exchanged with friends (Buchegger and Le Boudec, 2002c).

Path manager: It performs functions like path re-ranking according to security metric, path deletion containing malicious nodes and action to be taken on receiving request for a route from a malicious node.

Trust manager: It calculates trust levels, manages trust table entries for trust level administration, forwarding of alarm messages and filtering of incoming message based on the trust level of a reporting node.

Acknowledgement monitor module: The purpose of the acknowledgement monitor (Buchegger and Le Boudec, 2002a, b) module is to adjust the trust values from the received acknowledgements. Since, the trust values are used on routing selecting decisions, it is important that a missing acknowledgement is detected fast. When an

acknowledgement is received, it is reported to reputation system and trust manager so, that the trust values of corresponding node are adjusted for further actions. If a requested acknowledgement is not received, the packet is considered dropped, so the trust values should be adjusted in a negative way.

Confidant: Cooperation of Nodes: Fairness in Dynamic Adhoc Networks is proposed by Buchegger and Boudec (2002a, b) is an extension to DSR. This is based on selective altruism and utilitarianism. The misbehaving nodes are detected and isolated. Trust relationships and routing decisions are based on experienced, observed or reported routing and forwarding behavior of other nodes.

THE PROPOSED SCHEME: IMPROVED DSR PROTOCOL

Identification of relationships between Neighbors in an adhoc network: In an adhoc network, the relationship of a node i to its neighbor node j can be any of the following types (Raghavan *et al*., 2006).

Node i is a stranger to neighbor node j: Node i has never sent/received messages to/from node j. Their trust levels between each other will be very low. Any new node entering an adhoc network will be a stranger to all its neighbors. There are high changes of malicious behavior from stranger nodes.

Node i is an acquaintance to neighbor node j: Node i has sent/received few messages from node j. Acknowledgements are received in time. Their mutual trust levels are neither too low nor too high to be reliable. The chances of malicious behavior will have to be observed.

Node i is a friend to neighbor node j: Node i has sent/received plenty of messages to/from node j. The trust levels between them are reasonably high. Acknowledgements are communicated in time. Probability of misbehaving nodes may be very less.

The above relationships are represented as a Friendship table in each node of an adhoc network. Consider the node 1 in Fig. 1. The friendship table of node 1 is represented as shown in Table 1.

Trust estimator: Is used in each node to evaluate the trust level of its neighboring nodes. The trust Level is a function of various parameters like (Raghavan *et al*., 2006).

Table 1: Friendship table for node 1

Neighbors	Relationship
2	F
3	F
4	A
5	F
6	S
7	A

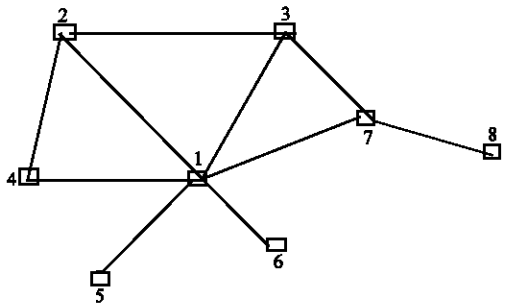

Fig. 1: Nodes in an adhoc network

- Length of the association.
- Ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor.
- Ratio of number of packets received intact from the neighbor to the total number of received packets from that node.
- Average time taken to respond to a route request.
- Acknowledgment received. If acknowledgment has been not received then there is every chance that particular node may be a malicious one.

The threshold trust level for a stranger node to become an acquaintance to its neighbor is represented by Tacq and the threshold trust level for an acquaintance node to become a friend of its neighbor is denoted by Tfri. The relationships are represented as:

$$R(n \rightarrow n) = F \text{ when } T \geq T_{fri}$$
$$R(n \rightarrow n) = A \text{ when } T_{acq} \leq T < T_{fri}$$
$$R(n \rightarrow n) = S \text{ when } 0 < T \geq T_{acq}$$

Also, the relationship between nodes is asymmetric, (i.e.,) R (n_i -> n_j) is a relationship evaluated by ni based on trust levels calculated for its neighbor nj. R (n_i -> n_j) is the relationship from the friendship table of node j. This is evaluated based on the trust levels assigned for its neighbor. Asymmetric relationships suggest that the direction of data flow may be more in one direction. In other words, node i may not have trust on node j the same way as node j has trust on node i or vice versa.

Table 2: Path chosen based on improved DSR

Next hop neighbor in the best path P1	Next hop neighbor in the next best path P2	Action taken
F	F	F is chosen in P1 or P2 based on the length of path
F	A	F is chosen in P1
A	F	F in path P2
A	A	A is chosen in P1 or P2 based on the length of the path
F	S	F is chosen in P1
S	F	F in path P2
S	S	S is chosen in P1 or P2 based on the length of the path
A	S	A or S is chosen on the length of the path
S	A	S or A base on length of the path

Routing mechanism: When any node wishes to send messages to a distant node, its sends the ROUTE REQUEST to all the neighboring nodes. The ROUTE REPLY obtained from its neighbor is sorted by trust ratings. The source selects the most trusted path. If its one hop neighbor node is a friend, then that path is chosen for message transfer. If its one-hop neighbor node is an acquaintance and if the one hop neighbor of the second best path is a friend choose F. Similarly, an optimal path is chosen based table (Buchegger and Le Boudec, 2002a) on the degree of friendship existing between the neighbor nodes.

The source selects the shortest and the next shortest path based on the Table 2. Whenever, a neighboring node is a friend, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between friends. If it is an acquaintance or stranger, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the adhoc network are friends.

The threshold parameters are design parameters. Simulation is to be carried out with suitable values or all the parameters and the threshold thrust levels so as to obtain optimum performance. There is a trade off between offering good security in adhoc networks and overall throughput of the network. Hence, choosing an optimal value is crucial for the good functioning of the network.

SIMULATION SET UP

In our simulations we use several performance metrics to compare the improved DSR protocol with the existing one. Studies of performance evaluations of routing protocols for mobile adhoc networks indicate that the following metrics are defined:

Packet delivery ratio: It is the ratio of the number of packets received and the number of packets sent.

Throughput: This gives the fraction of the channel capacity used for data transmission.

For the performance analysis of the protocol extensions, a regular well-behaved DSR network is used as a reference. We then introduce compromised stranger nodes into the network, which doesn't forward the packets. The network should identify these malicious nodes and not upgrade them to acquaintances. In the similar manner, some acquaintances are later made to be malicious. Simulations are carried out for the forwarding defection of the nodes. The simulation is being implemented In Network Simulator 2, a simulator for mobile adhoc networks.

Parameter	Value
Application traffic	CBR
Radio range	250 m
Packet size	512 bytes
Transmission rate	4 packets/s
Pause time for nodes	60 s
Maximum speed	1 m s^{-1}
Simulation time	600 s
Number of nodes	25
Area	1000 m * 1000 m
Available bandwidth	1 Mb s^{-1}

The speed of 1 m s^{-1} corresponds to slow moving. For a simulation that last 600 sec, approximately 30000 CBR packets are sent. This number is considered high enough to eliminate any deviations influence on the results. With 1 Mb/s bandwidth, a packet size of 512 bytes and a transmission rate of 4 packets/s, congestion of the network is not likely to occur.

For the performance analysis of the improved DSR protocol the throughput is compared with the standard DSR with malicious nodes. The other parameters to be considered are path optimality and routing overhead. Due to the introduced, acknowledgment scheme in the standard DSR number acknowledgement packets will be the overhead for the improved protocol. The Protocol is also tested based on the malicious drops over total drops in the network. The path optimality is another concern because when there is only choice of route containing the malicious nodes. As far as, number of alternative routes exists this protocol well works by choosing the optimal paths.

RESULTS

The improved DSR protocol is tested under different scenarios by varying the number of malicious nodes and node moving speed. It is also, tested varying the number of nodes in simulation used.

The packet delivery ratio is used to compare the existing DSR protocol and the modified DSR protocol to

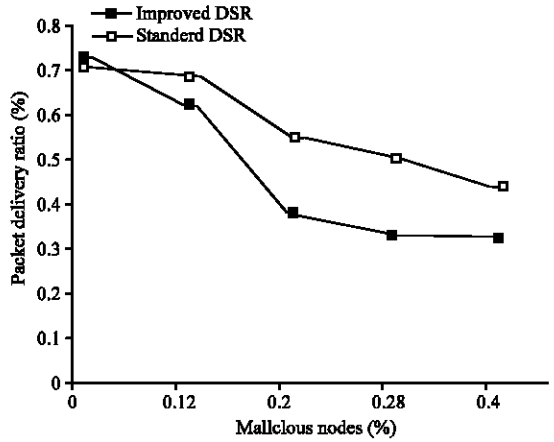

Fig. 2: Packet delivery ratio

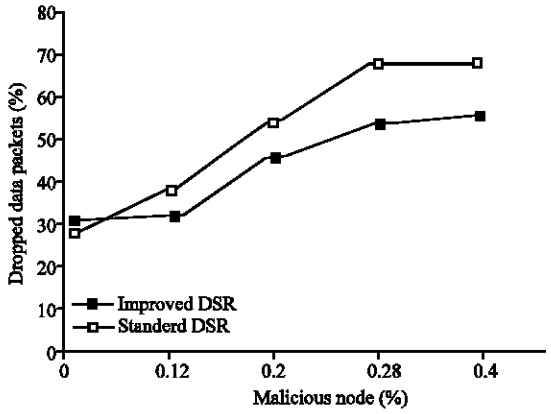

Fig. 3: Percentage of malicious drops over total drops

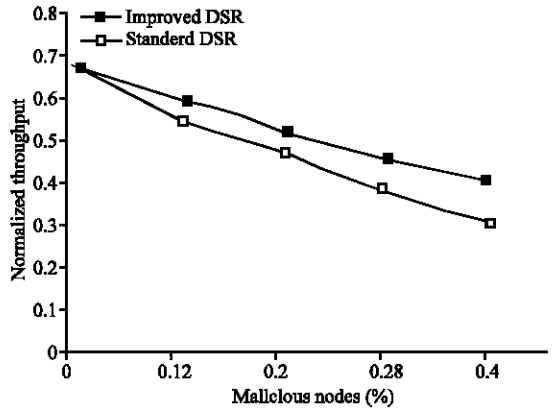

Fig. 4: Indicates the achieved throughput by improved DSR greater than the standard DSR

determine the influence of the trust based routing to the DSR protocol. The simulation results are presented in Fig. 2.

We carried out another simulation to determine the amount of packets that are dropped by malicious nodes from the total dropped packets. The simulation results are presented in Fig. 3. As the Fig. 4 illustrates, less packet drops are caused by malicious nodes during simulations for the improved DSR than for the existing DSR.

FUTURE WORK

For the purpose of simulation, we have assumed forwarding defection as the only possible misbehavior. The next step is to do performance analysis on the improved protocol by introducing possible attacks and further improvement in the protocol is to be done by changes in the extent of relationships used.

CONCLUSION

In this study, we have discussed the characteristics of mobile adhoc network and security challenges that it has to encounter. Although, MANET does not offer much contribution as wired networks, the suitability of MANET usage in a certain field such as in military battlefield and emergency situation is undeniable. Hence, it is important to always come out with more effective security mechanisms to protect MANET especially with its routing protocol. We presented the security enhancement for the existing DSR protocol by improving the concept of trust value calculation using battery power and acknowledgement monitor, for MANET routing. We performed simulation study using the ns-2 simulator to analyze the proposed protocol, comparing with the existing DSR protocol. The results show that the Improved DSR protocol can achieve higher packet delivery ratio and throughput than existing DSR when malicious nodes are presented in the network.

REFERENCES

Buchegger, S. and J.Y. Le Boudec, 2002a. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM international symposium on Mobile adhoc networking and computing. pp: 226-236. http://doi.acm.org/10.1145/513800.513828.

Buchegger, S. and J.Y. Le Boudec, 2002b. Nodes bearing grudges: Towards routing security, fairness and robustness in mobile adhoc networks. Proc. 10th Euromicro PDP (Parallel, Distributed and Network-based Processing), Gran Canaria, pp: 403-410. http://doi.ieeecomputersociety.org/ 10.1109/EMPDP. 2002.994321.

Buchegger, S. and J.Y. Le Boudec, 2002c. Cooperative routing in mobile adhoc networks: Current efforts against malice and selfishness. Proc. Mobile Internet Workshop. Informatik. Dortmund, Germany, pp: 513-517. http://dblp.uni-trier.de.

Dawkins, R., 1976. The selfish Gene. Oxford University Press, 1980 Edition.

Giuli, S.M.T.J., K. Lai and M. Baker, 2000. Mitigating routing misbehaviors in Mobile adhoc networks. Proc. 6th Ann. Int. Conf. Mobile Computing networking, Boston, MA, USA, ACM, pp: 255-265, http://doi.acm.org/10.1145/345910.345955.

Johnson, D., D. Maltz, Y. Hu and J. Jetcheva, 2001. The dynamic source routing protocol for mobile adhoc networks. Internet Draft, Internet Engineering Task Force, http://www.ietf.org/internetdrafts/draft-ietf.

Raghavan, V.N., N. Bhalaji and T.P.M. Labbai, 2006. Extended dynamic source routing protocol for the non co operating nodes in mobile adhoc networks. Int. J. Applied Mathe. Comput. Sci., 3 (1): 12-17. http://www.waset.org/ijamcs/v3/v3-1-3.pdf.