World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:2, No:10, 2008

# Extended Dynamic Source Routing Protocol for the Non Co-Operating Nodes in Mobile Adhoc Networks

V. Narasimha Raghavan, T. Peer Meera Labbai, N. Bhalaji, and Suvitha Kesavan

Open Science Index, Electronics and Communication Engineering Vol:2, No:10, 2008 publications.waset.org/3568/pdf

***Abstract*—**In this paper, a new approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate in an ad hoc environment. The extended 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 result indicates the achieved throughput by extended DSR is greater than the standard DSR and indicates the percentage of malicious drops over total drops are less in the case of extended DSR than the standard DSR.

***Keywords*—**Mobile Adhoc Networks, DSR, Grudger protocol, Nodes.

## I. Introduction

THE mobile ad hoc networks communicate in a self-organized way without depending on any fixed infrastructure. This leads to new vulnerabilities to attacks which are not known in wired networks. Most of the protocols assume only well-behaving nodes for multi-hop operation of the networks. But the mobile environment is broadly divided into three categories:

*Open* – There is no static infrastructure. Nodes of various types exist. Network structure is unknown and the key issue is the network throughput.

*Managed Open* – The network uses the existing infrastructure like certification servers, access points etc. The key issue may vary depending on the system accessed.

*Managed Hostile* – They come under the classic ad hoc networks where the key issue is confidentiality and security. They are applicable in war and disaster areas.

In these environments, the intentional non-cooperation is mainly caused by two types of nodes: selfish ones that want to save power and malicious nodes that are not primarily concerned with power saving but that are interested in attacking the network. The dependability of the routing system is addressed by prevention vs., detection and reaction mechanisms. The related work done on both mechanisms is briefed in Section 4.

The remainder of the paper this paper is organized as follows. Section 2 briefs about the additional security issues concerned with a mobile ad hoc network. Section 3 addresses on the security attacks. Section 4 details the related work done on the preventive vs. detection and reaction mechanisms to curb selfish and malicious behavior in ad hoc networks. Section 5 elaborates on the new approach to isolate selfish nodes based on friendship relation between the nodes. Section 6 gives an outline of the simulation works to be done. Section 7 and 8 concludes by pointing to possible future work.

## II. Special Security Issues in Mobile Ad-Hoc Networks

In addition to authentication, integrity, confidentiality, availability, access control and non-repudiation, the mobile ad hoc networks also raise the following issues as discussed in [1].

*Co-Operation and Fairness:*

Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application-specific trade-offs between security and resource consumption of the device. The selfish nodes may try to economize on their resources by not forwarding messages. With increase in the population of the selfish nodes, total non-collaboration with other nodes will result. The normal well-behaved nodes will be sufferers being deprived of their resources in addition to exploiting their resources. This is evident in a biological example used in [9].

*Location Confidentiality:*

The routing information, for example in a military application, itself can be equally important rather than the message content itself. The traceability of nodes, both a physical location and the tracking down of a node identity based on its routing traffic is also an important issue to be considered.

*No Traffic Diversion:*

The advertisement of the routes should be true reflection knowledge of the topology of the network. The nodes may rebel and misbehave by diverting the traffic in following ways:

Routing: Malicious nodes can attract unusual traffic to themselves by means of false routing advertisements. The bogus route that exhibits properties of a good route are preferred over real routes. These bogus routes can be made to stay longer in routing caches. The malicious nodes will actually forward the messages to the original intended destination so as not to raise suspicion. The information gathered this way is utilized for more sophisticated attacks.

Forwarding: Non-cooperating nodes may forward messages to their partners in collusion for analysis, disclosure or monetary benefits or may decide not to forward messages at all, thus boycotting communications.

Open Science Index, Electronics and Communication Engineering Vol:2, No:10, 2008 publications.waset.org/3568/pdf

Hence, it may be advantageous for the nodes not to co-operate in the network by remaining selfish and at times malicious. Increasing population of such nodes may lead to a steep drop in the network throughput and efficiency. The above stated security issues are to be considered in a mobile ad hoc network because of its characteristics like vulnerability of channels, nodes, absence of infrastructure and dynamically changing topology.

## III. Security Attacks in Ad Hoc Networks

Due to its inadequate infrastructure and organizational properties, ad hoc networks are vulnerable to many security threats. In this paper, we are concerned with the attacks on the routing schemes rather than physical attacks. Physical attack may involve a powerful transmitter broadcasting a constant noise in the used frequency. Such attacks are easy to detect. A skilled attacker may try to use the weakness in the algorithms and protocols. This sort of subtle attacks cannot be detected easily. Any attack on ad hoc networks can be categorized as passive or active attacks.

In a passive attack the malicious entity only listens to the traffic, without disturbing the network. In an active attack, the misbehaving node actively disturbs the normal operation of the network. In this section, we present the attacks using modification, impersonation and fabrication.

In the attacks using modification the malicious node announces better routes than the other nodes in order to be inserted in the ad-hoc network by changing the route sequence number, modified hop count and denial of service attacks. The DOS may be by changing the packet leaders in such a way that they don't reach the destination.

In the attacks using impersonation the malicious nodes usurps the identity of another node by spooling MAC address of other nodes.

In the attacks using fabrication the malicious node generates traffic to disturb the good operation of an ad-hoc network, by routing disruption like falsifying route error messages, corrupting routing state, routing table overflow attack, replay attack and black hole. *Routing loops* are used by the attackers which are non-optimal paths that travel through the same node more than once. A *black hole* attack is used by a malicious node which makes all the traffic travel through it by claiming to have the shortest route to all other nodes in the network. Then, instead of forwarding the packets, the malicious node simply drops it. A variant of this black hole is the *gray hole*, attack, which selectively transmits some packets and drops others.

Other attacks towards an adhoc network include partitioning and replay attacks. The network traffic is analyzed by the attacker, who later singles out any single node connecting different independent parts of the network. The attacker splits the network into two halves by isolating the node as illustrated in Fig. 1.

*Replay attacks* are attacks where the attacker replays the already sent packets to the network. If some reply route requests are replayed, the obsolete information may get stored in the routing table which might course some nodes to be unreachable. Another variant of reply attacks is the *wormhole attack.*

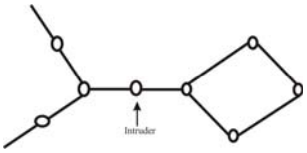



Fig. 1 Network Partitioning attack on a node in adhoc network

All of the problems presented in this section can severely harm the network. This may reduce the efficiency of the network and the network will function in a suboptimal way. If we are to transfer the data packets by using those nodes with high trust and reliability levels, then the purpose of formulating an adhoc network itself is defected. Also, congestion may occur in those paths. Hence, new routing schemes will have to be devised, taking all the above problems into considerations. Some of the related works and new secure routing schemas that are being developed are analyzed in section [4].

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.

## IV. Related Works

### *A. The Grudger Protocol*

As explained in [9] it is an application from a biological example proposed by Dawkins, which explains the survival chances of birds grooming parasites off each others head. Dawkins introduces three 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 ad hoc 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

Open Science Index, Electronics and Communication Engineering Vol:2, No:10, 2008 publications.waset.org/3568/pdf

maintained with friends and potentially exchanged with friends.

*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.

### *B. Other Related Works*

A *Security policy model* namely, *resurrecting duckling* suggested by Stajano and Anderson[7] describes a secure transient association of a device with multiple serialized owners. The authentication of users is done by 'imprinting' in reference to the ducklings recognizing the first moving object as their mother. During the imprinting phase, a shared secret is established between the duckling and the mother. Between the nodes in an ad hoc network, a symmetric encryption key is exchanged. The nodes can be imprinted several times. The address routing and forwarding of the messages is the future works to be addressed.

*Threshold Cryptography* and *diversity coding* schemes are introduced by Zhou and Haas [8] to build a highly secure network. Highly available key management service is established by distributing trust among a set of servers, employing share refreshing to achieve proactive security and adapting to changes in the network in a scalable way. The deployment of these security mechanisms in an ad hoc network and the impact of these security mechanisms on the network performance are to be considered.

A self-organized public-key infrastructure is developed by Hubaux, Buttyan and Capkum[2]. The certificate directories are stored and distributed by users. The *shortcut hunter algorithm* is proposed to build local certificate repositories for the users. Between any pair of users, they can find certificate chains to each other using only their local certificate repositories. New mechanisms are to be proposed if decentralization is introduced in self-organized mobile ad hoc networks.

A *secure routing protocol* (SRP) is presented by Papadimitratos and Haas [6]. This route discovery protocol mitigates the detrimental effects of such malicious behavior, so as to provide correct connectivity information. It guarantees that fabricated, compromised or replayed route replies would either be rejected or never reach back the querying node. Other features of this protocol include the requirement that the query verifiably arrives at the destination, the explicit binding of network and routing layer functionality, the consequent verifiable return of the query response over the reverse of the query propagation route, the acceptance of route error messages only when generated by nodes on the actual node, the query / reply identification by a dual identifier, the replay protection of the source and destination nodes and the regulation of the query propagation.

The routing misbehavior is mitigated by including components like *watchdog* and *pathrater* in the scheme proposed by Marti, Guiti, Lai and Baker[5]. Every node has a watchdog process that monitors the direct neighbors by promiscuously listening to their transmission. No penalty for the malicious nodes is awarded.

*Ariadne* is another secure routing scheme proposed by Hu and Perrig[4]. This routing protocol is designed to protect against active attackers. The routing security is achieved through digital signatures, TESLA authentication or by MAC authentication. TESLA authentication is based on hash key-chain and the nodes in the network should have synchronized clocks. Significant overhead is set up because authentication and confidentiality are required. Further, malicious nodes are not addressed here.

SEAD, *Secure Efficient Ad hoc Distance vector routing protocol* is proposed by Hu, Johnson and Perrig [3] which uses one way hash chains for authentication. This protocol is based on DSDV-SQ protocol. The routing messages like sequence number and path length are authenticated on a hop to hop hasis. Hence, malicious nodes cannot claim to have bogus links. In a mobile environment, there is a significant increase in overhead which may lead to congestion.

CONFIDANT *(Cooperation of Nodes: Fairness In Dynamic Ad hoc Networks)* is proposed by Buchegger and Boudec[1] 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 behaviour of other nodes.

## V. The Proposed Scheme : Extended DSR Protocol

### *A. Identification of Relationships between Neighbors in an Ad Hoc Network*

In an ad hoc network, the relationship of a node *i* to its neighbor node *j* can be any of the following types:

i. 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 ad hoc network will be a *stranger* to all its neighbors. There are high changes of malicious behavior from stranger nodes.

ii. node i is an *acquaintance* to neighbor node j

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

iii. 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. Probability of misbehaving nodes may be very less.

The above relationships are represented as a Friendship table in each node of an ad hoc network. Consider the node 3

Open Science Index, Electronics and Communication Engineering Vol:2, No:10, 2008 publications.waset.org/3568/pdf

in Fig 2. The friendship table of node 3 is represented as shown in Table I. A *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 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 and average time taken to respond to a route request.

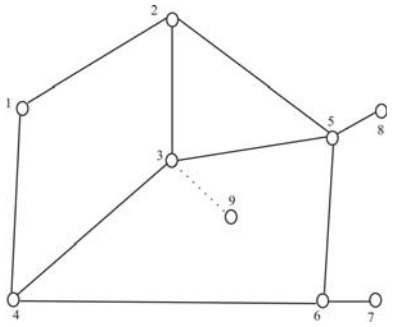



Fig. 2 Nodes in an Ad hoc Network

TABLE I
FRIENDSHIP TABLE FOR NODE 3 IN FIG.1

| Neighbors | Relationship |
|---|---|
| 2 | F |
| 4 | F |
| 5 | A |
| 9 | S |

The threshold trust level for a stranger node to become an acquaintance to its neighbor is represented by $T_{acq}$ and the threshold trust level for an acquaintance node to become a friend of its neighbor is denoted by $T_{fri.}$ The relationships are represented as

$$R(n_i \rightarrow n_j) = F \text{ when } T \geq T_{fri}$$

$$R(n_i \rightarrow n_j) = A \text{ when } T_{acq} \leq T < T_{fri}$$

$$R(n_i \rightarrow n_j) = S \text{ when } 0 < T < T_{acq}$$

Also, the relationship between nodes is asymmetric, (i.e, ) $R(n_i \rightarrow n_j)$ is a relationship evaluated by $n_i$ based on trust levels calculated for its neighbor $n_j$. $R(n_j \rightarrow n_i)$ is the relationship from the friendship table of node j. This is evaluated based on the trust levels assigned for its neighbor $n_i$. 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.

*B. 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 on the degree of friendship existing between the neighbor nodes.

TABLE II
PATH CHOSEN BASED ON EXTENDED DSR

| Next hop neighbor in the best path $P_1$ | Next hop neighbor in the next best path $P_2$ | Action Taken |
|---|---|---|
| F | F | F is chosen in P1 or P2 based on the length of path |
| F | A | F is chosen in $P_1$ |
| 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 $P_1$ |
| S | F | F in path P2. |
| S | S | S is chosen in $P_1$ 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 based on length of the path .. |

The source selects the shortest and the next shortest path. 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 ad hoc network are friends. Further the overheads due to the calculations of trust relationship are minimal compared to the CONFIDANT protocol. It will be slightly more than the normal DSR due to the invocation of the trust estimator whenever a data transfer is to be done through strangers or acquaintances.

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.

Open Science Index, Electronics and Communication Engineering Vol:2, No:10, 2008 publications.waset.org/3568/pdf

### C. Friends who Turn Malicious

Each node in an adhoc network would have identified its neighborhood friends over a certain period of time by evaluating their trust levels. Some of the neighborhood friends may suddenly turn malicious and non co-operative due to node capturing. To detect this, each node before starting the data transfer may invoke the trust evaluator for a specific interval of time and can reestablish the trust levels. If the threshold trust level is not satisfied, the friend is *degraded* to an acquaintance and their packets are not forwarded. This is the penalty the node pay for not being cooperative. If however, the node turns out to be a repenting offender that is no longer malicious and that has behaved normally for a certain amount of time, re-socialization or re-integration in to the network is possible if the threshold trust level for a friend is satisfied. In this case, the concerned node will have to work its way up to raise its trust level to the threshold set for a friend.

## VI. Simulation Set Up

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.

The simulations are carried out with 25 nodes moving with speeds 1 , 5 , 10 , 15 , 20 m/s in the region 670 X 670 and with connection patterns with 15 and 20 connections with pause time 10ms between the movement of nodes. The protocol is tested under these scenarios by varying the number of malicious nodes. The other scenarios are built by varying the number of nodes and the region which the nodes are going to be revolving around.

For the performance analysis of the extended 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 extended 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

## VII. Results

The extended 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 graph in Fig. 3 indicates the achieved throughput by extended DSR greater than the standard DSR.

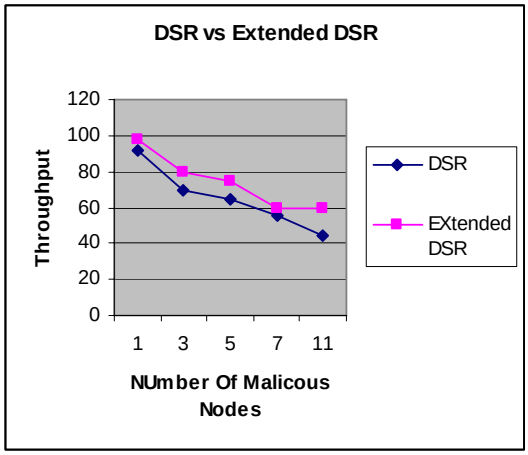



Fig. 3 Comparison of throughput achieved by extended DSR and DSR

The graph in Fig. 4 indicates the percentage of malicious drops over total drops. The percentages of malicious drops are less in the case of extended DSR than the standard DSR.

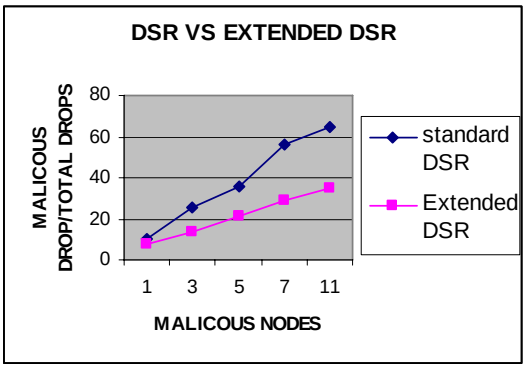



Fig. 4 Percentage of malicious drops over total drops

## VIII. 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 extended protocol by introducing possible attacks and further improvement in the protocol is to be done by changes in the extent of relationships used. Future work will be to evaluate and incorporate suitable solutions in the extended protocol.

## IX. Conclusion

Mobile adhoc networks exhibit new vulnerabilities to malicious attacks or denial of co-operation. Fairness mechanism is included by the notion of friends, acquaintances and strangers. The performance analysis by means of simulation is to be investigated, when DSR is fortified with the extensions. There will be a marginal increase in overhead with the use of the extended DSR protocol as far as the security concern that overhead will be negligible. As far as

number of alternative routes exists this protocol well works by choosing the optimal paths.

## REFERENCES

[1] Sonja Buchegger and Jean-Yves Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness and robustness in Mobile ad hoc networks. In *proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network–based processing,* Pages 403 – 410. Canary Islands, Spain. January 2002. IEEE Computer Society.

[2] Yih-Chun Hu, David.B.Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless ad hoc networks. In *proceedings of the 4th IEEE workshop on Mobile computing Systems & Applications (WMCSA 2002)*, IEEE, Calicoon.NY. to appear, June 2002.

[3] Yih-Chun Hu, Adrian Perrig, and David.B.Johnson. Ariadne: A secure on-Demand routing Protocol for ad hoc networks. Technical Report Technical Report TR01-383, Department of Computer Science, Rice University, December 2001.

[4] Sergio Marti.T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehaviour in Mobile ad hoc networks. In *Proceedings of MOBICOM 2000*. Pages 255-265, 2000.

[5] Frank Stajano and Ross Anderson. The resurrecting Duckling, Lecturer Notes in Computer Science, Springer – Verlag, 1999.

[6] Lidong Zhou and Zygmunt Haas. Securing ad hoc networks, In *IEEE Network Magazine*, special issue on networking security, Vol.13, No.6, November / December, Pages 24-30, 1999.

[7] Richard Dawkins. *The selfish Gene.* Oxford University press, 1980 edition, 1976.

[8] Sonja Buchegger and Jean-YvesLe Boudec. The selfish node: Increasing routing security for mobile ad hoc networks. IBM Research Report. RR 3354, 2001.

[9] Kai Inkinen. New secure routing in ad hoc networks: Study and Evaluation of proposed schemes. Seminar on Interworking HUT T-110.551.

Open Science Index, Electronics and Communication Engineering Vol:2, No:10, 2008 publications.waset.org/3568/pdf