World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:3, No:1, 2009

Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks

N. Bhalaji, A. R. Sivaramkrishnan, Sinchan Banerjee, V. Sundar, and A. Shanmugam

Abstract**—**Nodes in mobile Ad Hoc Network (MANET) do not rely on a central infrastructure but relay packets originated by other nodes. Mobile ad hoc networks can work properly only if the participating nodes collaborate in routing and forwarding. For individual nodes it might be advantageous not to collaborate, though. In this conceptual paper we propose a new approach based on relationship among the nodes which makes them to cooperate in an Adhoc environment. The trust unit is used to calculate the trust values of each node in the network. The calculated trust values are being used by the relationship estimator to determine the relationship status of nodes. The proposed enhanced protocol was compared with the standard DSR protocol and the results are analyzed using the network simulator-2.

Keywords**—**Reliable Routing, DSR, Grudger, Adhoc network.

I. Introduction

MOBILE ad hoc networks are paradigms for mobile communication[1] in which mobile nodes are dynamically and arbitrarily located in such a manner that communication between nodes does not rely on any underlying static network infrastructure. The communication medium is broadcast and the nodes in a mobile ad hoc network are usually portable mobile devices with constrained resources, Such as power, computation ability and storage capacity. Since no fixed infrastructure or centralized administration is Available, these networks are self-organized and end-to-end communication may require routing information via several intermediate nodes. Due to the lack of infrastructure and the limited transmission range of a node in a mobile ad hoc network, a node has to rely on neighbor nodes to route a packet to the destination node. In particular, all network functions are based on the node cooperation. Currently, routing protocols for mobile ad hoc network, such as the Dynamic Source Routing (DSR) [2] and the Ad hoc On Demand Distance Vector Routing Protocol (AODV) [3] are based on the assumption that all nodes will cooperate. Without node cooperation, in a Mobile ad hoc network, no route can be established; no packet can be forwarded, let alone any network applications. However, cooperative behavior, such as forwarding other node's messages, cannot be taken for granted. We can identify two types of uncooperative nodes: faulty or malicious and selfish. Faulty/malicious behavior refers to the broad class of Misbehavior in which nodes are either faulty and therefore cannot follow a protocol, or are intentionally malicious and try to attack the system. Selfishness refers to noncooperation in certain network operations. In mobile ad hoc networks, the main threat from selfish nodes is Drop ping of packets (black hole), which may affect the performance of the network severely. Both Faulty/malicious nodes and selfish nodes are misbehaved nodes. Due to the ad hoc nature of mobile ad hoc networks, enforcing cooperation in such networks is particularly challenging. The unique characteristics of mobile ad hoc networks raise certain requirements for the security mechanism.

N. Bhalaji is Research scholar in Anna university Coimbatore, India (corresponding author, phone: + 91-9884818049).

Siva, Sinchan, Sundar are associated with department of computer science, Srm university, Chennai, India.

A. Shanmugam is working as a principal in Bannari Amman institute of Technology, Sathyamangalam, Erode, India.

A. Organization of the Paper

The remainder of this paper is organized as follows. Security issues and type of attacks are discussed in the sections 2 and 3. Related work is discussed in Section 4, followed by a description of the proposed Trust Enhanced DSR protocol in Section 5. The simulation setup and corresponding results are outlined in section 6 & 7. Future work is outlined in Section 8 and conclusions are drawn in Section 9.

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.

Co-Operation and Fairness

Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application-specific tradeoffs 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 [4].

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 good routes is 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. Hence, it may be advantageous for the nodes not to cooperate 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.

Apart from the security issues discussed above the adhoc network is also vulnerable to many kinds of attacks which are discussed in the next section.

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 [5] the malicious entity only listens to the traffic, without disturbing the network. In an active attack [6], the misbehaving node actively disturbs the normal operation of the network. In this section, we present the attacks using modification, impersonation [7] 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* [8] are used by the attackers which are non-optimal paths that travel through the same node more than once. A *black hole* [8] *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* [9], 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. *Replay attacks* [5] 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* [10]. 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 schemes that are being developed are analyzed in the following sections.

In this proposed scheme using Trust Enhanced 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 Work

A. DSR Protocol

Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks and was proposed for MANET by Broch, Johnson, and Maltz [2]. 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.

B. The Grudger Protocol

As explained in [4] [11] 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.

C. Watchdog and Pathrater

The routing misbehavior is mitigated by including components like *watchdog* and *pathrater* in the scheme proposed by Marti, Guiti, Lai and Baker [12]. 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.

D. CONFIDANT (Cooperation of Nodes: Fairness in Dynamic Ad hoc Networks)

The CONFIDANT protocol works as an extension to reactive source routing protocols like DSR [13]. The basic idea of the protocol is that nodes that does not forward packets as they are supposed to, will be identified and expelled by the other nodes. Thereby, a disadvantage is combined with practicing malicious behavior. The protocol consists of four components.

V. The Proposed Scheme

This section presents the improvement of the Trust Enhanced Route selection to be applied to the DSR protocol in order to strengthen the security of the routing protocol. In contrast to the process of route selection in the DSR protocol which selects the shortest route to the destination, in our proposed protocol we choose the most reliable and secure route to the destination based on the trust values of all nodes.

- For each node in the network, a trust value will be stored that represent the value of the trustiness to each of its neighbor nodes. This trust value will be adjusted based on the experiences that the node has with its neighbor nodes.
- When a node receives data packets or acknowledgements from its neighbor node, the trust value for this neighbor node will be upgraded. Neighbor node that is encountered for the first time will have an initial trust value assigned based on trust formation strategy. If a route contains known nodes, the trust values of these neighbor nodes are used to base the assignment of the initial trust value.
- If a requested acknowledgement was not received, the trust value for this neighbor node should be decreased.

A. Components of the Proposed Protocol

The proposed protocol consists of the following components [14].

1. Trust Unit
    1.1. Initialiser
    1.2. Upgrader
    1.3. Administrator
2. Monitor
3. Router

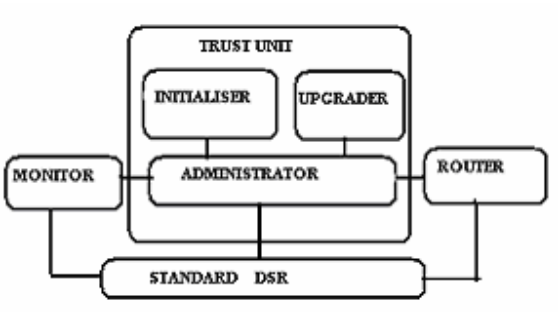

Fig. 1 Components of Trust Enhanced DSR

Trust Unit

***Initialiser Module*:** This module is used to assign a trust value for unknown new mobile nodes in the network. It would be best to assign a low trust value in an environment with many malicious nodes. If a route contains known nodes, the trust value of these nodes is used to base the assignment of the initial trust value for the new node.

Upgrader Module: The upgrader module of trust unit is used to implement the Functions for upgrading trust. The updating of the trust values will depend on a given node experience in a given situation. We use the following function to upgrade the trust value for each node encountered in the route the function for upgrading trust depends on two parameters, previous trust values and the experience values:

*Tu(Ev,Tv) = (1-C) *E + C*Tv*
Where
Tu: The upgraded trust value
Tv: The existing trust value
Ev: The experience value
C: A constant to express the inflation of trust

The experience value consists of knowledge of the Acknowledgements received and data packets received.

Administrator: The Administrator module of the trust unit stores trust information about all known nodes during run time, and it offers methods to query for information about stored trust values. So it is used as the interface between the existing DSR protocol on one hand and the Initialiser and Upgrader modules on the other hand.

Router: The route selector module is responsible to evaluate routes based on the Relationship status of nodes which in turn depends on the trust values of nodes in each route; and selects the best route based on this evaluation. The routes are evaluated and a route with the good Relationship (Friend) is then selected. This means that the best route will be considered as one that has the highest trust rating, which means that it has the lowest number of malicious nodes.

Monitor: The purpose of the monitor 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, the trust upgrader module upgrades the trust values for nodes on the stored route. If a requested acknowledgement is not received, the packet is considered dropped, so the trust values should be adjusted in a negative way.

B. Nature 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 have 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. High changes of malicious behavior from stranger nodes.

ii. node i is an acquaintance to neighbor node j

Node i have 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 have 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 Relationship table in each node of an ad hoc network. Consider the node 1 in Fig 2. The Relationship table of node 1 is represented as shown in Table I. A *Relationship estimator is* used in each node to evaluate the trust level of its neighboring nodes. The relationship estimator checks the trust level from the administrator module of trust unit and decides the relationship status of each node based on the threshold value. The methods of threshold fixation are discussed below.

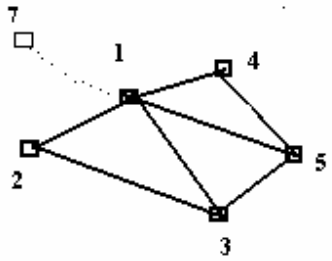

Fig. 2 Nodes in an Ad hoc Network

TABLE I
RELATIONSHIP TABLE FOR NODE 1 IN FIG. 2

Neighbors	Relationship
2	F
3	F
4	A
5	F
7	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 (node i → node j) = F when $T \geq T_{fri}$

R (node i → node j) = A when $T_{acq} \leq T < T_{fri}$

R (node i → node j) = S when $0 < T \geq T_{acq}$

Also, the relationship between nodes is asymmetric, (i.e.,) R (node i → node j) is a relationship evaluated by node i based on trust levels calculated for its neighbor node j. R (node j → node i) 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.

C. 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 PROPOSED SCHEME

Next hop neighbor in the best path P1	***F***	F	A	***A***	S
Next hop neighbor in the best path P1	A	***F***	***F***	S	***F***

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.

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.

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 do not 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[15], 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 750 X 500 and with connection patterns with 15 and 20 connections with pause time 10ms between the movements 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 Trust enhanced DSR, the throughput is compared with the standard DSR in presence of malicious nodes. The other parameters to be considered are path optimality and routing overhead. The routing overhead will be high in the proposed protocol but it can be neglected in view point of security.

Due to the introduced acknowledgment scheme in the standard DSR number acknowledgement packets will be the overhead for the proposed 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 Trust Enhanced 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. For the performance analysis we consider parameters like throughput, packet delivery ratio and total number of drops/Malicious nodes. The standard DSR protocol and the proposed protocol are the exposed to the above said attacks and its performance are plotted in a graph as shown below.

The graph in Fig. 2 indicates the achieved throughput by Trust Enhanced DSR greater than the standard DSR.

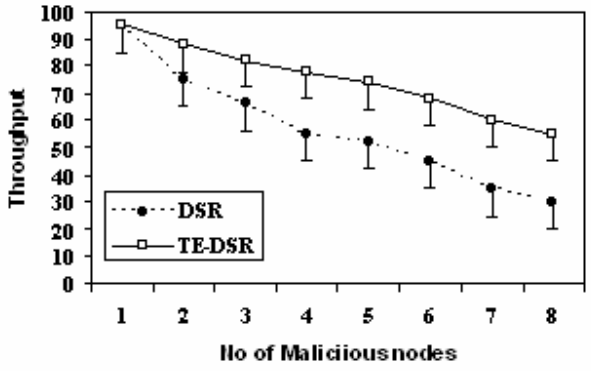

Fig. 2 Comparison of throughput

The graph in Fig. 3 indicates the percentage of malicious drops over total drops. The amount of malicious drops is less in the case of Trust Enhanced DSR than the standard DSR.

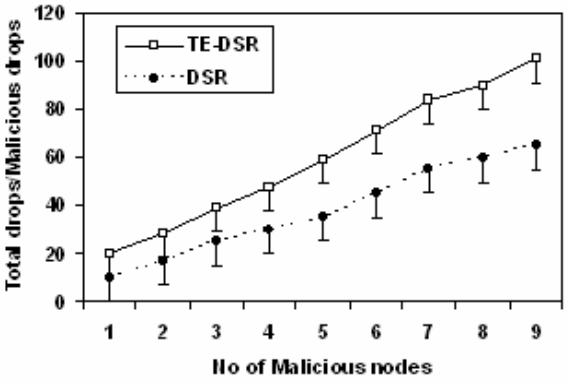

Fig. 3 Comparison of malicious drops over Total drops

The next parameter considered for the simulation was packet delivery ratio. It also plays a significant role in performance of the protocol. The graph in Fig. 4 indicates the comparison of Packet Delivery Ratio vs. No of Malicious nodes.

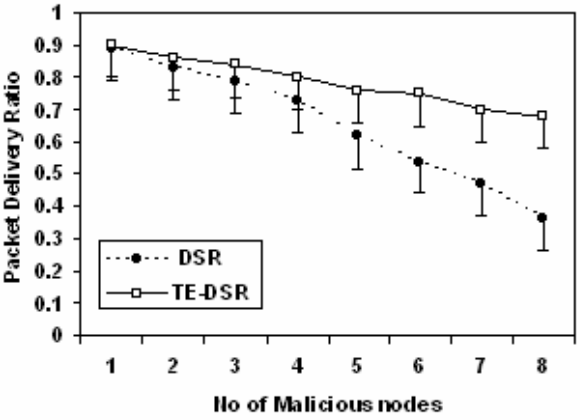

Fig. 4 Comparison of Packet Delivery Ratio

The routing overhead is high in proposed protocol when compared with the standard DSR. But it is not given much importance and accepted at the cost of improved performance of the proposed protocol.

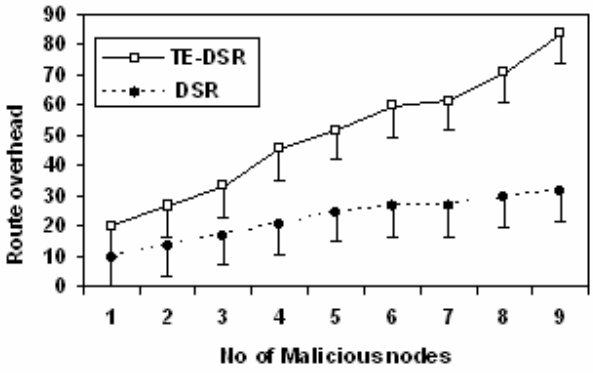

Fig. 5 Comparison of Routing Overhead

VIII. Future Work

The paper represents the first step of our research to analyse the packet dropping attack over the proposed scheme to analyse its performance. The next step will consist of analyzing the protocol over different types of attack which we have discussed in section 2 of this paper.

IX. Conclusion

In this paper we have discussed the characteristics of mobile adhoc network. We also analyzed the different types of issues and attacks in an adhoc environment. This proposed scheme of Trust Enhanced DSR protocol increases the level of security routing and also encourages the nodes to cooperate in the adhoc structure. It identifies the malicious nodes and isolates them from the active data forwarding and routing.

References

[1] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols" Prentice Hall, 2004.

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

[3] C.E.Perkins and E.M.Royer "Ad hoc on demand distance vector routing", Proceedings of IEEE Workshop on Mobile computing systems and Applications 1999, pp. 90-100, February 1999.

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

[5] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy May/June 2004.

[6] S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, October 2002. https://forum.eviloctal.com/redirect.php?tid=1992&goto=lastpost.

[7] Adam Burg, "Ad hoc network specific attacks ", Seminar on Ad hoc networking: concepts, applications, and Security, Technische Universität München, 2003.

[8] P. Papadimitratos, and Z.J. Haas, "Securing the Internet Routing Infrastructure," IEEE Communications, vol. 10, no. 40, October 2002, pp. 60-68. Digital Object Identifier 10.1109/MCOM.2002.1039858

[9] Ernesto Jiménez Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem" TKK T-110.5290 Seminar on Networksecurity2006-12-11/12. www.tml.tkk.fi/Publications/C/22/papers/jimenez_final.pdf

[10] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks," Proc. 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03), San Francisco, CA, April 2003, ISSN: 0743-166X, INSPEC Accession Number: 7853884. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1209219.

[11] 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

[12] 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.

[13] Sonja Buchegger and Jean-Yves Le Boudec: "Performance analysis of the CONFIDANT protocol" Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing'02. p.p:226 – 236. http://doi.acm.org/10.1145/513800.513828.

[14] John Keane, "Trust-based Dynamic Source Routing in Mobile Ad Hoc Networks", MS thesis, Department of Computer Science, Trinity College Dublin, September 2002.

[15] Kevin Fall, Kannan Varadhan: The ns manual, http://www.isi.edu/nsnam/ns/ doc/index.html