Reliable Routing against Selective Packet Drop Attack in DSR based MANET

N.Bhalaji
Research Scholar, Anna University Coimbatore,
Tamilnadu, India. Ph: 91 44 2226 0923
Email: bhalaji.80@gmail.com

Dr.A.Shanmugam
Principal, Bannari Amman institute of Technology,
Tamilnadu, India.
Email: dras_bit@yahoo.com

Abstract— **a mobile ad hoc network (MANET) is a self-organizing, self-configuring confederation of wireless systems. MANET devices join and leave the network asynchronously at will, and there are no predefined clients or server. The dynamic topologies, mobile communications structure, decentralized control, and anonymity creates many challenges to the security of systems and network infrastructure in a MANET environment. Consequently, this extreme form of dynamic and distributed model requires a revaluation of conventional approaches to security enforcements. In this paper, we propose a new routing mechanism to combat the common selective packet dropping attack. Associations between nodes are used to identify and isolate the malicious nodes. Simulation results show the effectiveness of our scheme compared with conventional scheme.**

Keywords— **Reliable Routing, Association based DSR, Selective packet dropping attack, malicious nodes, Adhoc network**

I. INTRODUCTION

Mobile ad hoc networks have received great attention in recent years, mainly due to the evolution of wireless networking and mobile computing hardware that made possible the introduction of various applications [1]. Mobile nodes communicate using wireless interfaces without a fixed network infrastructure. In these environments each node may act as source or as a router. Nodes that cannot communicate directly depend on their neighbours in order to forward their messages to the appropriate destination. Applications of mobile ad hoc networks have increased requirements in order to ensure high quality of service for the provided services. Security in such infrastructure-less networks has been proven to be a challenging task. Many security threats arise against mobile ad hoc networks, as they are inherently vulnerable due to the way the build and preserve connectivity characteristics. The open medium presents the network with the first and most serious vulnerability. Unlike wired networks where an aggressor in order to launch an attack has to gain access to a wired infrastructure, firewalls and gateways, in ad hoc networks there is no clear line of defence. Every node is vulnerable and the good performance of the network depends on every node or at least on every node participating in a path from the source to a given destination. The insecure open medium combined with poor physical protection presents another disadvantage. Each node is able to roam independently running the risk to be easily compromised by a malicious attacker. Furthermore, when more sophisticated attacks take place nodes can be easily exploited. In addition, wireless ad hoc networks lack a centralized monitoring and management point.

II. BACK GROUND

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 neighbours, 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.

Since DSR has no security mechanism malicious nodes can perform many types of attacks just by not behaving properly according to DSR rules. This article provides routing security to the DSR protocol by eliminating the threat of selective packet drop attacks.

B. Common Security Threats

The nodes of a MANET are actually mobile routers that build up routes dynamically. These routers can move randomly and insert themselves automatically into dynamic wireless topologies. They perform packet forwarding using the current routing information. A path form the source to the destination, that is, a route, can be established through well known routing protocols such as the ad hoc on-demand distance vector routing (AODV, [3]), dynamic source routing (DSR, [2]), temporally ordered routing algorithm (TORA, [4]), zone routing protocol (ZRP, [5]), and destination-sequenced distance-vector (DSDV, [6]). Selfish and malicious nodes take advantage of Manet's idiosyncrasies to misbehave, or attack. As far as the MANET is concerned, the following types of attacks have been reported:

Impersonation or spoofing: Such an attacker will try to spoof a node that resides in the route of the data Flow of interest [7]. Such an attack can be materialized since the conventional routing protocols (e.g., AODV, DSR, TORA, and ZRP) do not support authentication of IP addresses. A similar threat is called *Sybil attack* [8]. An attacker does not only impersonate one node, but it assumes the identity of several nodes, and, thus, undermines the redundancy of many routing protocols [9].

Sinkhole: where an attacker tries to attract all the data sent by its neighbours. This attack is the basis for example, eavesdropping [9]. Sinkhole attackers present themselves to adjacent nodes as the most attractive relay in a multi-hop route.

Wormhole: where a malicious node uses a path outside the MANET (tunnel) to forward packets to another, colluding, node in the fixed network [10]. According to [10], the route discovery methods of on-demand routing protocols are violated by avoiding the normal route and by forwarding the RREQ packets directly to the destination.

Routing fabrication: where an attacker tampers with the normal routing procedures. It is achieved through alteration of the routing messages' fields (e.g., poisoning of DSR routing caches) or by the insertion of false routing messages (e.g., falsifying route error messages). Routing 'fabrication' produces denial-of-service (DoS) and partitioning of a MANET. In [11] several threats are identified, which are materialized through the modification of the routing messages' fields, such as modified sequence number, hop counts, or source route.

DoS and flooding: They are considered as indirect results of the aforementioned attacks [9]. A direct DoS attack, introduced in [12], is the sleep deprivation torture. One node, or colluding nodes, continually request the services offered by the target node. This consumes the battery of the target, which goes into an idle or power preserving state.

C. Selective packet dropping attack

A selective packet drop is a kind of denial of service where a malicious node attracts packets and drops them selectively without forwarding them to the destination. As an example consider the scenario in figure 1. Here node 1 is the source node and node 7 is the destination node. Nodes 2 to 6 acts as the intermediate nodes. Node 5 acts as a malicious node. When source wishes to transmit data packet, it first sends out RREQ packets to the neighbouring nodes. The malicious nodes being part of the network also receives the RREQ. The source node transmits data packets after receiving the RREP from the destination. As node 5 is also the part of routing path will receive the data packets and drops some of them while forwarding others. This type of attack is very hard to detect as the malicious nodes pretend to act like a good node.

The selective packet dropping attacks have a great negative influence over the performance metrics of conventional protocols. In this article we propose a dynamic trust based approach to combat selective packet drop attacks.

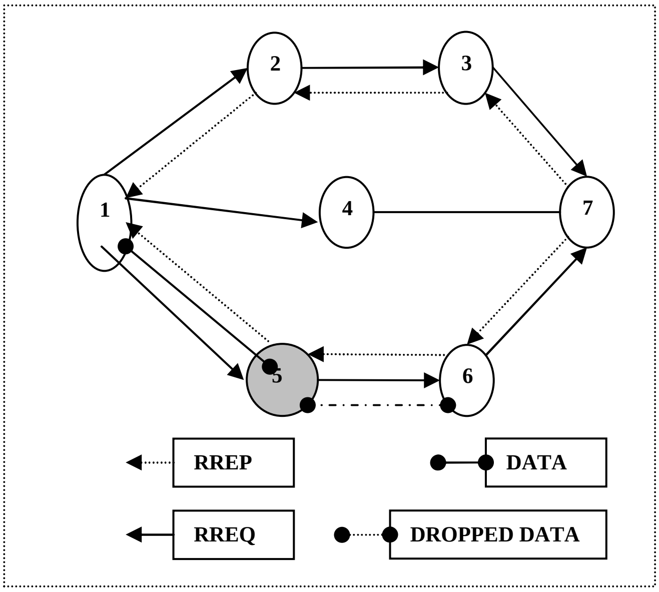

Figure. 1. Selective Packet drop attack scenario

III. RELATED WORK

Misbehaviour detection and reaction are described in [13], by Marti, Giuli, Lai and Baker. The paper presents two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission. This technique is imperfect due to collisions, limited transmit power and partial dropping. However, according to simulations [9], it is highly effective in source routing protocols, such as DSR. The path rater uses the knowledge from the watchdog to choose a path that is most likely to deliver packets. The path rating is calculated by averaging the rating of the nodes in the path, where each node maintains a rating for all the nodes it knows in the network. Watchdog is used intensively in many solutions for the cooperation problem. The main drawback of this idea is that it enables selfishness and misbehaving nodes to transmit packets without punishing them, and thus encourages misbehaviour.

Buchegger and Le Boudec [14] present the CONFIDANT protocol .Each node Monitor the behaviour of its next hop neighbours in a similar manner to watchdog. The information is given to the reputation system that updates the rate of the nodes. Based on the rating, the trust manager makes decisions about providing or accepting route information, accepting a node as part of a route and so on. When a neighbour is suspicious in misbehaving, a node informs its friends by sending them an ALARM message. If a node’s rating turns out to be intolerable, the information is relayed to the path manager, which proceeds to delete all routes containing the intolerable node from the path cache. This does not address partial packet dropping.

Michiardi and Molva propose the CORE scheme and various related issues in [15] [16]. In this scheme, every node computes a reputation value for every neighbour, based on observations that are collected in the same way as watchdog. The reputation mechanism differs between subjective reputation, indirect reputation, and functional reputation. Subjective reputation is calculated directly from neighbours past and present observations, giving more relevance to past observations in order to minimize false detection influence. Indirect reputation is the information collected through interaction and information exchange with other nodes using positive values only. Functional reputation is the global reputation value associated with every node. By avoiding the spread of negative rating, the mechanism resists attacks, such as denial of service. When a neighbour reputation falls below a predefined value, the service provided to the misbehaving node is suspended.

The Grudger Protocol As explained in [17] 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 favour others by grooming parasites off others head.
- Cheats which get help from others but fail to return the favour.
- Grudger who starts out being helpful to every bird, but bears a grudge against those birds that don’t return the favour and subsequently no longer help them.

In an ad hoc network, grudger nodes are introduced which employ a neighbourhood watch by keeping track of what is happening to other nodes in the neighbourhood, before they have a bad experience themselves. They also share information of experienced malicious behaviour with friends and learn from them.

A. Other related work

A *Security policy model* namely, *resurrecting duckling* suggested by Stajano and Anderson [18] 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 [19] 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 [20]. 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 [21]. This route discovery protocol mitigates the detrimental effects of such malicious behaviour, 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.

Ariadne is another secure routing scheme proposed by Hu and Perrig [22]. 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 keychain 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 [23] 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 basis. 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.

In all the above works there is no significant proposal to safeguard the adhoc network against the selective packet drop attacks.

IV. THE PROPOSED SCHEME

This section presents the extension of Association based routing which is to be applied over the DSR protocol in order to enhance the security. The purpose of this scheme is to fortify the existing implementation by selecting the best and secured route in the network. For each node in the network, a trust value is calculated which represent its reliability level. Based on the trust value calculated and threshold parameters they are classified in to three types as discussed below.

A. Nature of Association between neighbouring nodes in an Ad Hoc Network

In our proposed scheme we classify the Association among the nodes and their neighbouring nodes in to three types as below. In an adhoc network the Association between any node **x** and node **y** will be determined as follows.

UNKNOWN

- Node x have never sent/received any messages to/from node y
- Trust levels between them are very low.
- Probability of malicious behaviour is very high.
- Newly arrived nodes are grouped in to this category.

KNOWN

- Node x have sent/received some messages to/from node y
- Trust levels between them are neither low nor too high.
- Probability of malicious behaviour is to be observed.

COMPANION

- Node x have sent/received plenty of messages to/from node y
- Trust levels between them are very high.
- Probability of malicious behaviour is very less.

The above Associations are represented in an Association table which is part of every node in the adhoc network. For an example the Association table of node 1 in the fig.2. Is given in Table 1.

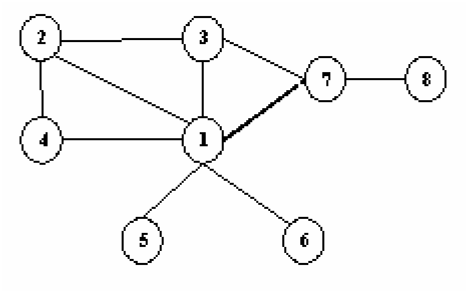

Figure 2. Nodes in Adhoc network

TABLE I
Association Table for node 1 in Fig. 2

Neighbours	Nature of Association
2	C
3	C
4	K
5	C
7	UK

B. Association estimator technique

The Association status which we discussed in the previous section depends up on the trust value and threshold values. The trust values are calculated based on the following parameters of the nodes. We propose a very simple (1) for the calculation of trust value between any two node in the network.

$$\mathbf{TV = \tanh (R1+R2+A)} \quad \ldots \quad (1)$$

Where

TV = Trust value

$$\mathbf{R1} = \frac{\text{No. of packets forwarded successfully by neighbour node}}{\text{Total no of packets to be forwarded by neighbour node}}$$

If the denominator is not zero and R1 is less than the chosen threshold (R1<1) & not zero then it can cause selective packet drop attack.

$$\mathbf{R2} = \frac{\text{No. of packets received from neighbour node But originated from other nodes}}{\text{Total no of packets received from that node}}$$

A = Acknowledgement. (0 or 1) if the acknowledgment is received for data transmission from the destination then nodes in that path are assigned value 1 else value 0 is assigned.

The threshold trust level for an unknown node to become a known to its neighbour is represented by T_K and the threshold trust level for a known node to become a companion of its neighbour is denoted by T_C. The Associations are represented as

A (node x → node y) = Companion, if $T \geq T_C$

A (node x → node y) = Known, if $T_K \leq T < T_C$

A (node x → node y) = Unknown, if $0 < T > T_K$

Where T = Threshhold
K = known,
UK= unknown,
C = companion

Also, the Association between nodes is asymmetric, (i.e.,) R (node x → node y) is an Association evaluated by node x based on trust levels calculated for its neighbour node y. R (node y → node x) is the Association from the friendship table of node y. This is evaluated based on the trust levels assigned for its neighbour. Asymmetric Associations suggest that the direction of data Flow may be more in one direction. In other words, node x may not have trust on node y the same way as node y has trust on node x or vice versa.

The Threshold parameters are design parameters. Simulation is to be carried out with suitable values or all the parameters and the threshold trust 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.

C.Routing Mechanism

When any node wishes to send messages to a distant node, its sends the ROUTE REQUEST to all the neighbouring nodes. The ROUTE REPLY obtained from its neighbour is sorted by trust ratings. The source selects the most trusted path. If its one hop neighbour node is a Companion, then that path is chosen for message transfer. If its one-hop neighbour node is a known, and if the one hop neighbour of the second best path is a companion choose C. Similarly an optimal path is chosen based on the degree of Association existing between the neighbour nodes.

TABLE II
Path Chosen Based On Proposed Scheme

Next hop neighbour in the best path P1	Next hop neighbour in the next best path P2	Action Taken
C	C	C is chosen in P1 or P2 based on the length of path
C	K	C is chosen in P1
K	C	C in path P2
K	K	K is chosen in P1 or P2 based on the length of the path
C	UK	C is chosen in P1
UK	C	C in path P2
UK	UK	UK is chosen in P1 or P2 based on the length of the path
K	UK	K or UK is chosen on the length of the path
UK	K	UK or K based on length of the path

C = companion, K= known, UK = unknown

The source selects the shortest and the next shortest path. Whenever a neighbouring node is a companion, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between companions. If it is a known or unknown, 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 companions.

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 known or unknown

V. SIMULATION SET UP

The simulation is implemented In Network Simulator 2 [29], a simulator for mobile adhoc networks. The simulation parameters are provided in Table 3.

TABLE III
Simulation parameter

Parameter	Value
Examined Protocol	DSR
Application traffic	CBR
Transmission range	250 m
Packet size	512 bytes
Transmission rate	4 packets/sec
Pause time	10 s
Maximum speed	20 m/s
Simulation time	900 s
Number of nodes	50
Area	1000 m * 1000 m
Propagation Model	Free space
Maximum Malicious nodes	20
Movement Model	Random waypoint
Types of attack	Selective packet drop

A. Mobility Model

We implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen between 0 m/s to the maximum simulation speed. A packet size of 512 bytes and a transmission rate of 4 packets/s, congestion of the network are not likely to occur.

VI. RESULTS AND DISCUSSIONS

For the performance analysis of the Association based DSR protocol the throughput is compared with the standard DSR in presence of the malicious nodes. The other parameters [30] to be considered are packet delivery ratio and dropped data packets.

Performance Metrics In our simulations we use several performance metrics to compare the proposed DSR protocol with the existing one. The following metrics were considered for the comparison were

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.

Average Latency: Gives the mean time (in seconds) taken by the packets to reach their respective destinations

Byte Overhead: This is the ratio between the total numbers of control bytes generated to the total number of data bytes received during the simulation time.

Fig. 3 depicts the performance results for the DSR protocol in the presence of malicious nodes. The results indicate that the throughput of the protocol rapidly drops with the increase in the number of malicious nodes. The throughput drops in DSR rapidly when the number of malicious nodes increases.

Fig. 4. Shows the percentage of packet delivery ratio under the threat of increasing malicious nodes. Here too the proposed protocol performs better than the conventional one.

We conducted another simulation to determine the percentage of dropped data packets for proposed and standard protocol. When no malicious nodes are present the standard DSR has less dropped data packets but these changes when the number of malicious nodes increases. The results are shown in Fig. 5

The simulation results in Fig 6. & Fig.7 illustrates that the average latency and byte over head are slightly higher than the conventional one due to the trust based routing.

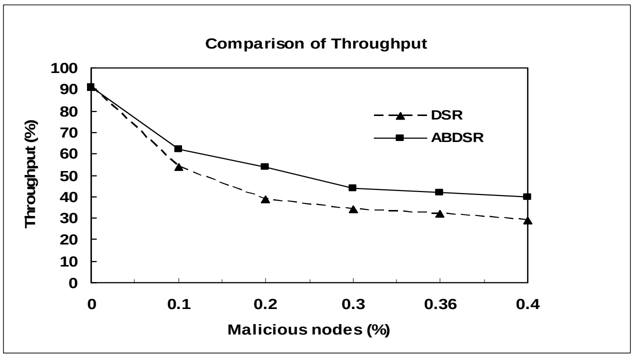

Figure 3. Throughput

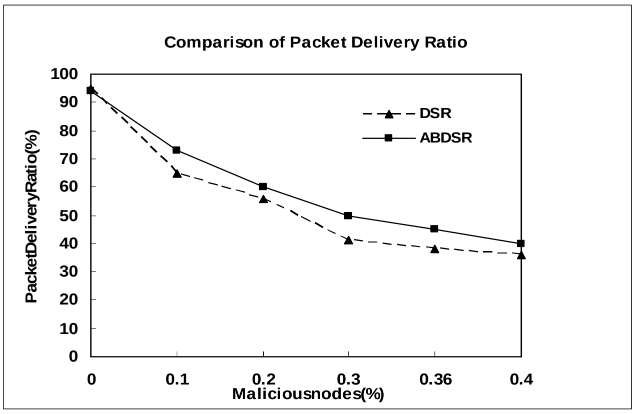

Figure 4. Packet delivery Ratio

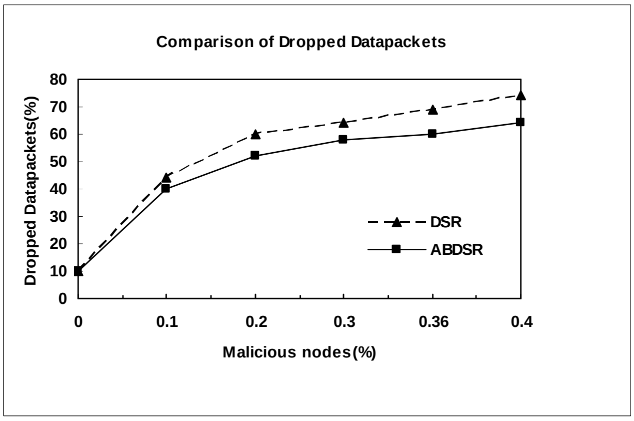

Figure. 5. Dropped data packets

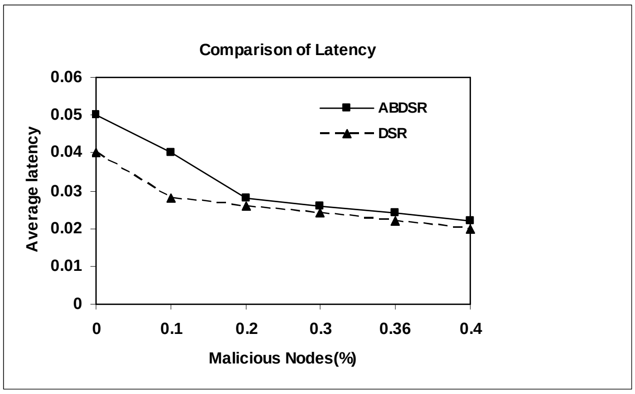

Figure. 6. Dropped data packets

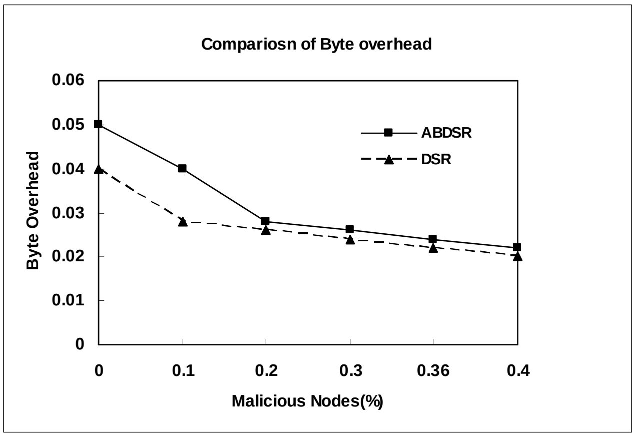

Figure 7. Byte overhead

VI. CONCLUSION

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 imposes certain unessential requirements, which are considered as restrictive for unplanned environments. In this paper we have discussed the dynamic trust based approach through which association between nodes are used to resist selective packet drop attacks connected to adhoc networks. With the help of the Network simulator we were able to prove that the proposed scheme increases the routing security and encourages the nodes to cooperate in the adhoc structure. Our scheme is equipped with technique to identify and isolate the malicious nodes 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]. Johnson DB, Maltz DA. "Dynamic source routing in ad hoc wireless networks. In Mobile Computing" *Imielinski T, Korth H (Eds). Kluwer Academic Publishers*: Boston, 1996; 153–181.

[3]. Perkins CE, Royer EM. "Ad-hoc on-demand distance vector routing" *Proceedings of 2nd IEEE Workshop on Mobile Computer Systems and Applications,* February 1999.

[4]. Park VD, Corson MS. "A highly adaptive distributed routing algorithm for mobile wireless networks" *Proceedings of IEEE INFOCOM'97*, April 1997.

[5]. Haas ZJ. "A new routing protocol for the reconfigurable wireless networks" *Proceedings of IEEE 6th International Conference on Universal Personal Communication*, October 1997.

[6]. Perkins CE, Bhagwat P "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers" ACM *SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications,* August 1994.

[7]. Karlof C, Wagner D. "Secure routing in wireless sensor networks: Attacks and countermeasures*" Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Applications* May 2003.

[8] Douceur J. "The sybil attack" *Proceedings of 1st International*
Workshop on Peer-to-Peer Systems (IPTPS02), March 2002.

[9] Burg A. "Ad hoc network specific attacks" Seminar *Ad hoc networking: Concepts, Applications, and Security. Technische Universitat* Munchen, '03.

[10] Hu YC, Perrig A, Johnson DB. "Packet leashes: A defence against wormhole attacks in wireless ad hoc networks" Technical Report TR01-384, Department of Computer Science, Rice University, December 2001.

[11]. Michiardi P. "Cooperation enforcement and network security mechanisms for mobile ad-hoc networks" *Ph. D. thesis, Ecole nationale supe´rieure des telecommunications*, December 2004.

[12] Jøsang A. "The right type of trust for distributed systems" *Proceedings of ACM New Security Paradigms Workshop,* September 1996.

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

[14]. 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

[15] P. Michiardi and R. Molva. Preventing denial of service And selfishness in adhoc networks. In Working Session on Security in Ad Hoc Networks, Lausanne, Switzerland, June 2002.

[16] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of the 6th IFIP Communications and Multimedia Security Conference, pages 107–121, Portorosz, Slovenia, September 2002.

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

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

[19] 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.

[20] J.Hubaux, L.Buttyan, and Sc.Capkun. The quest for security in Mobile Ad hoc Networks. In *proceedings of the ACM Symposium on Mobile Ad hoc Networking and Computing* (MobiHOC) 2001

[21] Papadimitratos P, Haas ZJ, Samar P. "The secure routing protocol (SRP) for ad hoc networks" *Proceedings of the 2nd ACM workshop on Wireless security*, San Diego, CA, USA, Pages: 41 - 50 2003.

[22] Hu YC, Perrig A, Johnson DB. "Ariadne: a secure on-demand Routing protocol for ad hoc networks" *Proceedings of 8th ACM International Conference on Mobile Computing and Networking*, September 2002.

[23]. Hu YC, Johnson DB, and Perrig A. "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks" *Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications*, June 2002.

[24] J. Broch, D. Johnson, D. Maltz, Y. Hu, J.Jetcheva, "A Performance Comparison of Multihop Wireless Ad Hoc Networking Protocols", *Proceedings of 4th ACM/IEEE International Conference on Mobile Computing and Networking*, 1998

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