CHAPTER 4

A NOVEL ROUTING SCHEME TO COMBAT PACKET DROPPING ATTACKS IN MANETs

4.1 INTRODUCTION

The main assumption of the ad hoc routing protocols is that all participating nodes do so in good faith and without maliciously disrupting the operation of the dynamic source routing protocol. However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like ad hoc networks. The RPSEC IETF working group has performed a threat analysis that is applicable to routing protocols employed in a wide range of application scenarios (Murphy 2002). Cryptographic solutions can be employed to prevent the impact of attackers by mutual authentication of the participating nodes through digital signature schemes (Zhang 1998). However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level. The nodes which do not send the received packets (used for storing battery life span to be used for their own communications) are called selfish nodes (Kong 2002). A selfish node (Blasevic et al 2001) impacts the normal network operations by not participating in routing protocols or by not sending packets.
4.2 PACKET DROPPING ATTACK MODEL

The selfish node does not perform the packet forwarding function. When this behaviour is selected, the packet forwarding function performed by the Nodes are disabled for all packets that have a source address or a destination address different from the current selfish node. However, a selfish node that operates following this model participates in the route discovery and route maintenance phases of the DSR protocol. As an example consider the scenario in Figure 4.1.

![Figure 4.1 Packet Dropping Attack Scenario](image)

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. The consequence of the proposed model in terms of consumed energy is that the selfish node will save a significant portion of its battery life
neglecting data packets, while still contributing to the network maintenance. This chapter focuses on nodes which do not forward but drop packets and it is believed that the selfishness problem receives more attention in mobile ad hoc network as the nodes are battery-powered. Thus energy is a precious resource that they may not want to waste for the benefit of other nodes.

4.3 RELATED WORK

The routing misbehavior is mitigated by including components like watchdog and pathrater in the scheme proposed by Marti et al (2000). Every node has a watchdog process that monitors the direct neighbors by promiscuously listening to their transmission. Main draw back of this idea is that it enables the misbehaving node to participate in the network cooperation without punishing.

Buchegger and Boudec (2002) present a reputation based protocol, called CONFIDANT, for making misbehavior unattractive (Murthy and Garcia 1996). CONFIDANT stands for Cooperation of Nodes: Fairness in Dynamic Ad-hoc Network, it works as an extension to on demand routing protocols. CONFIDANT aims at detecting and isolating uncooperative nodes, thus making it unattractive to deny cooperation. Reputation is used to evaluate routing and forwarding behavior according to the network protocol. Trust is used to evaluate participation in the CONFIDANT meta-protocol. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes. With CONFIDANT, each node has the following four components: a monitor, a trust manager, a reputation system and a path manager. These components interact with to provide and process protocol information. The monitor is the equivalent of a neighbor watch", where nodes locally monitor deviating behavior. A node can detect deviation by its neighbor on the source route by listening to the
transmission of its neighbor. The monitor reports any suspicious events and any incoming ALARM messages to the trust manager. The trust manager makes decisions about providing or accepting route information, accepting a node as part of a route, or taking part in a route originated by another node. It consists of the following components:

- An alarm table containing information about received alarms.
- A trust table managing trust levels for nodes to determine the trustworthiness of an alarm.
- A friends list containing all the ‘friends’ that the node may send alarms to.

ALARM messages contain the type and frequency of protocol violations, are sent by the trust manager of a node to warn others of uncooperative nodes. Outgoing ALARM messages are generated by the node itself after having experienced, observed, or received a report of uncooperative behavior. The recipients of these ALARM messages are so-called friends, which are administered in a friends list. Incoming ALARM messages are originated from either outside friends or other nodes, and the source of an ALARM has to be checked for trustworthiness before triggering a reaction.

The reputation system in this protocol manages a table consisting of entries for nodes and their rating. The rating is changed only when there is sufficient evidence of uncooperative behavior that is significant for a node and has occurred a number of times exceeding a threshold to rule out coincidences. To avoid a centralized rating, local rating lists and/or black lists are maintained at each node and potentially exchanged with friends.
The path manager performs the following functions:

- Path re-ranking according to reputation of the nodes in the path.
- Deletion of paths containing uncooperative nodes.
- Action on receiving a request for a route from an uncooperative node (e.g. Ignore, do not send any reply).
- Action on receiving request for a route containing an uncooperative node in the Source route (e.g. ignore, alter the source).

Each node monitors the behavior of its neighbors. If a suspicious event is detected, the information is given to the reputation system. If the event is significant for the node, it is checked whether the event has occurred more often than a predefined threshold that is high enough to distinguish deliberate uncooperative behavior from simple coincidences such as collisions. What constitutes a significant rating can be determined for different types of nodes according to their security requirements. If a certain threshold is exceeded, the reputation system updates the rating of the node that caused the event. If the rating turns out to be intolerable, the information is relayed to the path manager, which proceeds to delete all routes containing the misbehaving node from the path cache.

Buchegger et al (2002) improved the CONFIDANT protocol to cope with false disseminated reputation information. A trust rating is introduced to represent the trustworthiness of a node. In addition to reputation rating, each node also maintains a trust rating for every other node. Only second hand reputation information that is from a trusted node and is compatible with the current reputation rating will be accepted. A Bayesian approach is used to evaluate both reputation rating and trust rating.
The CONFIDANT protocol works as an extension to reactive source routing protocols like DSR. 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, if a node is found to be intolerable then all the routes which consists of this node will be deleted.

The Grudger Protocol (Buchegger and Boudec 2002) is an application from a biological example proposed by Richard Dawkins (1980) which explains the survival chances of birds grooming parasites off each others head. Dawkins introduces three categories of the birds namely suckers, cheats, grudger. 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 Security policy model namely, resurrecting duckling suggested by Stajano and Anderson (1999) 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.

Threshold Cryptography and diversity coding schemes are introduced by Zhou and Haas (1999) 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 et al (2001). 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 (Blazevic et. al. 2001) mobile ad hoc networks.

A secure routing protocol (SRP) is presented by Papadimitratos et al (2003). 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.

Ariadne is another secure routing scheme proposed by Yih-Chun Hu et al (2005). 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 et al (2002) 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.
The Authenticated Routing for Ad-hoc Networks (ARAN) (Dahill et al 2002) secure routing protocol relies on the use of digital certificates and can successfully operate in the managed-open scenario where no network infrastructure is pre-deployed, but a small amount of prior security coordination is expected. ARAN requires the use of a trusted certificate server in the network. This requirement imposes a number of pre-setup restrictions that must be catered to before establishing the ad-hoc network. Also, having a centralized certificate repository in a physically insecure environment creates a single point of compromise and capture.

4.4 SIMULATION ENVIRONMENT

The simulation is implemented in Network Simulator-2 (Fall and Kannan 2003), a simulator for mobile adhoc networks. The Dynamic Source Routing protocol is used for analysing the proposed scheme. Simulate the network with 1000m*1000m space and 50 mobile nodes. The simulation time is 900seconds. The random waypoint movement model is implemented for the simulation with a maximum speed of 20m/s the pause time is 10seconds, which represents a network with moderately changing topology. The communication pattern used is constant bit rate (CBR). In random way model 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. 20 selfish nodes are assumed in each of the simulation, which is almost more than 40 percent of total nodes.

4.5 PERFORMANCE ANALYSIS

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 (Broch et al 1998) to be considered are packet delivery ratio and dropped data packets.

4.5.1 Packet Delivery Ratio

Figure 4.2 depicts the performance results for the DSR protocol in the presence of malicious nodes. The results indicate that the packet delivery ratio of the protocol rapidly drops with the increase in the number of malicious nodes. When 30% of the nodes turn into packet droppers then the packet delivery ratio achieved by the conventional DSR is about 40% whereas for the same percentage of malicious nodes the proposed DSR is able to provide 50% of the successful packet delivery. When the 40% of the nodes are exhibiting the packet dropping behaviour the packet delivery ratio achieved by the standard DSR is 32% whereas for the Association based dynamic source routing protocol. Thus approximately 10% increase in total packet delivery is achieved which is very significant in ad hoc environments.

Figure 4.2 Packet Delivery Ratios of the DSR and ABDSR in Presence of Varying Packet Dropping Nodes
4.5.2 Throughput

Figure 4.3 shows the percentage of throughput under the threat of increasing malicious nodes. Here too the proposed protocol outscores the conventional one. Both the standard DSR and proposed ABDSR obtain 91% of throughput when no attackers are found in the simulation. But it degrades gradually as the number of attackers increase in the simulation. The DSR protocol without the proposed scheme achieves only 26% of the throughput under the maximum number of malicious nodes whereas the proposed ABDSR scores 36% for the above said scenario. Thus considerable improvement is obtained by using the proposed scheme.

Figure 4.3 Throughputs of the DSR and ABDSR in Presence of Varying Packet Dropping Nodes

Another simulation to determine the percentage of dropped data packets for proposed and standard protocol is conducted. 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 Figure 4.3.
4.5.3 Total Drop

The total drop in the DSR under attack is 10% higher than the proposed DSR Protocol, this is achieved by the former that does not take into account the benevolent nature of nodes and prefers shortest path. Attacking nodes are selected constantly in the routing process, which leads to reduced throughput and packet delivery ratio. The proposed DSR protocol, on the other hand, regularly monitors the behavior of its nearby nodes, it selects route nodes depending on their association status thus tries to avoid attacking nodes.

![Graph showing dropped data packets of DSR and ABDSR](image)

**Figure 4.4** Dropped Data Packets of the DSR and ABDSR in Presence of Varying Packet Dropping Nodes
4.5.4 Average latency and Byte Overhead

The simulation results in Figures 4.4 and 4.5 illustrate that the byte overhead and average latency which are slightly higher than the conventional one due to the trust based routing.

Figure 4.5 Average Latency of the DSR and ABDSR in Presence of Varying Packet Dropping Nodes

Figure 4.6 Byte overhead of the DSR and ABDSR in Presence of Varying Packet Dropping Nodes
4.6 CONCLUSION

Mobile ad hoc networks are commonly targeted by participating malicious node to attack the network. Many experiments have shown that techniques like cryptography, hashing, authentication are not enough and implementation of those techniques imposes certain unessential requirements. In order to combat the dynamic nature of Manet, in this section the association based approach by enforcing trust between the nodes is implemented. Each node in the network will monitor its surrounding neighbours and based on certain criteria decides the nature of association between them. This enhances the nodes to select the reliable routes instead of standard shortest route. The simulation results prove that 10% increase in throughput and packet delivery ratio is achieved by the proposed novel based routing scheme in the presence of packet dropping attackers.