An Analysis of Routing Disruption Attack on Dynamic Source Routing Protocol

Jaydip Sen
Innovation Lab, Tata Consultancy Services Ltd.
Bengal Intelligent Park, Salt Lake Electronic Complex
Kolkata 700091, INDIA
Email: Jaydip.Sen@tcs.com

Abstract—Dynamic Source Routing (DSR) is a well known source routing protocol for ad hoc networks. The algorithm depends on the cooperative participation of the nodes that enables route discovery from a source node to a destination node. However, if a group of nodes do not cooperate, the performance of the DSR protocol may be severely degraded. This paper presents a probabilistic attack model on the DSR protocol and analyses its effect on the routing performance. Simulations results of the model show that the effect of the attack is catastrophic only if a large number of nodes are compromised and there is no detection mechanism. As an interesting observation, the analysis also shows that the attack model can also be used to improve the performance of the DSR protocol.

Keywords—mobile ad hoc network, dynamic source routing, packet dropping attack, route request, route reply, route error.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless hosts that can be rapidly deployed as a multi-hop packet radio network without the aid of any established infrastructure or centralized administrator. Such networks can be used to enable next generation of battlefield applications, including situation awareness systems for maneuvering war fighters, and remotely deployed unmanned micro-sensor networks. MANETs have some special characteristic features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are absent or less severe in wired networks. MANETs are vulnerable to various types of attacks. These include passive eavesdropping, active interfering, impersonation, and denial-of-service. Intrusion prevention measures such as strong authentication and redundant transmission can be used to improve the security of an ad hoc network. However, these techniques can address only a subset of the threats, and in addition, they are costly to implement.

Due to lack of an infrastructure in a MANET, each node operates both as a host as well as a router. There are several ad hoc routing protocols proposed in the literature [1][2][3]. However, none of them consider any security issues. In fact one of the most critical problems in MANETs is the security vulnerabilities of the routing protocols [4]. A set of nodes in a MANET may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network.

Among ad hoc routing protocols, ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) are accepted as experimental standards by the IETF MANET working group.

In this paper, a routing disruption attack on the DSR protocol is presented, where a group of attacker nodes do not re-broadcast route request packets and do not send cached replies with a probability $P$. The extent of the attack depends on the number of attacking nodes in the network and the attack probability $P$. The rationale of the attacker behind applying the attack in a probabilistic way and not dropping all the route request packets is that it makes more difficult for any mechanism to detect the attacker.

The feasibility of the attack is primarily investigated from the point of view of the attacker and the requirement of a defense mechanism to reduce the negative effects of the attack using a combination of analytical and simulation studies. It has been observed that it is possible to reduce the negative effects of the attack on the route discovery process by employing a detection mechanism.

As another important observation, while investigating the effects of the attack model on DSR protocol, it is realized that the success ratio of the route discovery process does not degrade significantly until the attack probability exceeds a certain threshold. This gives us an idea that there might be an optimum probability for the legitimate nodes to re-broadcast route requests. In this way, network utilization can be improved by decreasing the number of broadcasts flooded in the network.

The rest of the paper is organized as follows: In Section II, an overview of the DSR protocol is given. Section III provides a brief summary of the related work existing in the literature. Section IV describes a routing disruption attack on the DSR protocol. Section V presents an analytical model for the attack. Section VI provides the simulation results on the attack scheme, and Section VII concludes the paper.
II. DYNAMIC SOURCE ROUTING PROTOCOL

DSR is a routing protocol designed for mobile wireless ad hoc networks [1]. In an ad hoc network that uses DSR protocol, each data packet follows a route that is discovered and maintained by a source node and this route is included in the header of all data packets from source to destination. There are two main mechanisms in the DSR protocol: Route Discovery and Route Maintenance.

A. Route Discovery

When a source node wants to send a packet to a destination node, it first queries its Route Cache where the previously discovered routes are kept. If no route is found in its cache, source node initiates route discovery process to find a new route to the destination node.

In route discovery process, source node broadcasts a route request packet, which is received by all nodes within the wireless transmission range of source. Each route request message carries the identifications of the source and the destination nodes’ unique request identification and a list of the addresses of the intermediate nodes through which that route request packet has been forwarded.

When the destination node receives this route request message, it returns a route reply message to the source node containing the path taken by the route request message. When the source node receives this route reply message, it caches the path in its route cache in order not to repeat route discovery process for each new packet destined to the same target node.

If the node receiving the route request message has recently seen another route request message from the same source node with the same request identification and destination address or if the address of this node is already listed in the route path of the route request message, this node discards the received route request message. Otherwise, the node appends its own address to the route path record of the route request message and broadcasts it with the same request identification.

![Figure 1. Route Discovery Example](image)

Fig. 1 depicts an example route discovery scenario. Node 1 would like to transmit a packet to node 8 and none of the nodes has a route to node 8 in their cache. A request packet is broadcast from node 1 and received by nodes 2, 3 and 4. They append their addresses to the request packet and rebroadcast the message. Since nodes 2, 3 and 4 have just processed the request, they will discard the re-transmitted request from each other. Although, node 5 receives from 2 and 3, it will discard the request from node 2 since it received the same request from node 3 previously. Node 7 receives the request from node 5; adds its address and re-broadcasts. On the other hand, node 6 receives the request from node 4 and rebroadcasts it. Node 8 receives the request from node 6 and discards any future receptions with the same request, such as the request from node 7. The route between nodes 1 and 8 is established as 1-4-6-8.

B. Route Maintenance

Broadly speaking, route maintenance is achieved by acknowledgment mechanism in DSR. Every node ensures that data flows from one node to the next one by requesting acknowledgments. A node not receiving acknowledgment will transmit acknowledgment requests for a certain period of time. If no acknowledgment has been received, then the sender treats the link as broken. In such a case, the sender removes this link from its Route Cache and returns a route error packet to the previous node in the route. The route error packet propagates all the way back to the source node, and each node on the route removes the broken link from their route cache.

III. RELATED WORK

A number of works have been done on the area of ad hoc network security especially for detection of packet dropping attacks by malicious nodes. This section mentions some of these works.

To solve the problem of reduction in the throughput due to selfish and malicious nodes in a MANET, Marti et al. proposed two additional components to the dynamic source routing protocol (DSR): watchdog and pathrater [5]. When a node forwards a packet, the node’s watchdog verifies whether the next node in the path also forwards the same. The watchdog does this by listening promiscuously to the next node’s transmissions. If the next node does not forward the packet, then it is misbehaving. The pathrater assesses the results of the watchdog and selects the most reliable path for packet delivery. However, this scheme has several drawbacks. First of all, overhearing does not always work particularly in situations like collisions or weak signals. Secondly, pathrater actually does not punish malicious nodes that do not cooperate in routing. Rather it relieves them of the burden of forwarding packets for others, while their messages are forwarded without any problem. In this way, the malicious nodes are rewarded and reinforced in their behavior.

CONFIDANT protocol proposed by Buchegger et al. extends the concepts of watchdog and pathrater [6]. In this mechanism, misbehaving nodes are not only excluded from forwarding route replies, but also from sending their own route request. The scheme includes a trust manager to evaluate the level of trust of alert reports and a reputation system to rate each node. The reports from trusted sources are only processed by the nodes. However, it is not clear how fast the trust level can be adjusted for a compromised node especially if it has a high trust level initially.

Buttyan et al. have advocated the use of tamper-resistant hardware on each node of a MANET to encourage cooperation [7]. Nodes are assumed to be unwilling to forward packets unless they are stimulated to do so. In this approach, a
protected credit counter runs on the tamper-resistant device. It increments by one when a packet is forwarded. It refuses to send its own packets if the counter is smaller than a threshold. Public key cryptography is used to exchange credit counter information among the neighbors and verify if forwarding is really successful. However, the availability of tamper-resistant hardware is a very vital assumption for the successful working of the scheme that involves complexity in hardware design.

Sen has proposed an approach for detection of malicious packet dropping attack on MANETs that brings out the complementary relationship between key distribution and misbehavior detection [8]. The redundancy of routing information is utilized for developing a protocol that works even in presence of transient network partitioning and Byzantine failure of nodes.

Sun et al. have presented a framework to quantitatively measure trust, model trust propagation, and defend trust evaluation system against malicious attacks [9]. The attacks against trust evaluation are identified and defense techniques have been proposed.

Chang et al. have proposed a trust-based scheme for multicast communication in a MANET that involves a two-step secure authentication method [10]. In the first step, an ergodic continuous Markov chain is used to determine the trust value of each one-hop neighbor. In the next step, the node with the highest trust value is selected as the certificate authority (CA) server.

The redundancy caused by broadcasting in ad hoc networks has been analyzed and various types of broadcast mechanisms have been proposed in order to reduce redundant message transmission [11]. In [12], a probabilistic broadcasting mechanism is presented that performs well in a dense ad hoc network.

IV. ROUTING DISRUPTION ATTACK ON DSR

Since ad hoc networks lack infrastructure, every node is potentially a router in the network. This adds much vulnerability to the routing protocol. Specifically, there are many attacks to which DSR is vulnerable. Some of these attacks may target data packets such as DoS with modified source routes and route cache poisoning [4].

However, most of the attacks against a routing protocol target the routing packets exchanged among nodes. By spoofing, altering or dropping routing information, attackers may be able to create black holes [4], increase routing traffic or end-to-end latency, and even partition the network.

A. Attack Model

As briefly discussed in Section II, nodes process route requests by sending back cached route replies or by re-broadcasting route requests in DSR route discovery phase while dropping the redundant route requests. A possible attack against route discovery mechanism of DSR is to capture a node and not process route request packets arriving at that node. In the rest of the paper, we focus on a variation of this type of attack. The attack scenario is envisaged as follows:

When an attacker who has captured a normal node receives a route request packet, it checks if there exists a route to the destination in the route cache. If such a route exists, in contrast to normal nodes, it does not send a cached route reply with a probability of $P$, i.e., it sends the route reply with probability $1-P$. If there is no cached route to the destination, in contrast to normal nodes, attacker does not rebroadcast this route request with the same probability $P$. In other words, the attacker rebroadcasts with probability $1-P$.

Long term controlled attacks can be considered much more destructive than short-term sudden attacks. Therefore, attackers aim to disrupt the route discovery with the maximum effect without being detected. This is necessary for the continuity of the attack.

The aim of the attack model is to prevent route discovery for the overall ad hoc network. If there is no mechanism that detects routing disruption attacks, attacker may simply compromise as many nodes as it can and apply the attack with probability of 1, i.e., drop all route request packets. The reason why the attacker applies the attack in a probabilistic way is to hide against any detection mechanism that can detect a routing disruption attack. The attacker will not be detected until he compromises a certain number of nodes and/or increases the attack probability. These threshold values are analyzed in Section VI. However, the mechanisms that can be used to detect the attacker in the network are out of scope of this paper.

Such an attack appears quite plausible in a hostile environment. The attack model assumes that the attacker has captured legitimate and operational nodes so that he is able to access all of the facilities of those nodes with normal user’s rights and privileges. Even if the route discovery process is secured with encryption and authentication measures, the attacker may still physically capture the node and prevent route reply and rebroadcast of the route requests. An encryption or authentication measure can not prevent this type of an attack.

The proposed attack that limits re-broadcasting the route request packets is not able to stop the route discovery process altogether. This is because of the redundant characteristic of the broadcast mechanism, i.e., when there are two or more nodes in the transmission range of the broadcast. For this reason, the proposed attack model will not be able to disrupt the overall network route discovery until a certain number of nodes are compromised.

The effects of the number of compromised nodes in the network and the route request dropping probability on the overall success of route discovery are analyzed in Section V and Section VI.

V. ANALYTICAL MODEL

A probabilistic model is proposed to analyze the effects of the attack on route discovery mechanism. The following parameters are used in the model. $N$ is the average number of nodes per route. $R$ is the average number of paths returned for the same route request and for the same source-destination pair. $P$ is the probability of not re-broadcasting, i.e., attack probability. $\alpha$ is the ratio of the number of compromised nodes...
to the total number of nodes in the network, i.e., the probability that a node is compromised.

A node re-broadcasts (or returns a route reply) with probability $1 - P$ if it is compromised, and with probability 1 if it is not compromised. Thus, the probability that all the nodes on a path with average length $N$ will re-broadcast the route-request or return the route reply from their cache is given by $[\alpha(1 - P) + (1 - \alpha)]^N$. It also gives the probability for a path to be connected. The probability of at least one of the nodes on a path with average length $N$ will not re-broadcast the route request packet is denoted by $P_0$ and given by (1)

$$P_0 = 1 - [\alpha(1 - P) + (1 - \alpha)]^N \quad (1)$$

$P_0$ is also the probability of this path to be broken. Since there are $R$ different paths to the destination and the compromised nodes behave independently on deciding to re-broadcast or not, it is assumed that each of the paths has a probability of $P_0$ of being broken. Thus, the overall probability of all of the paths being broken, route discovery failure probability $P_R$, is given as follows.

$$P_R = [1 - (\alpha(1 - P) + (1 - \alpha))]^N \quad (2)$$

By estimating the values of $N$ and $R$, the attackers can utilize (2) to find out the attack probability ($P$) value for his desired route discovery failure probability. Such an analysis is given in Section VI.

The attackers may determine $R$ and $N$ values by a short-term routing traffic analysis of the network. This can also be implemented as a self-training mechanism allowing dynamic update of the re-broadcast probability.

VI. EXPERIMENTAL RESULTS

Simulations are performed in the network simulator ns-2. A network consisting of 100 static nodes is considered for the purpose of simulation. The routing algorithm used is DSR and nodes are running multiple FTP sessions from an FTP server.

Fig. 2 shows that on average, the number of route replies is six times the number of route requests when there is no attacker in the network. Using this information, the value of $R$ (number of paths) can be estimated as six for the simulated network. Also, Fig. 2 suggests that the average number of nodes per route is four, i.e. $N = 4$. These values are used for analysis in the analytical model given in Section V.

The change of $P_R$ with respect to $P$ for the simulated network is illustrated in Fig. 3 for different values of $\alpha$. The equation (2) is used for this analysis. For the simulated network $P_R$ is very low for $\alpha = 0.1$ and $\alpha = 0.2$, even if the attack probability $P$ is 1. Significant damage on the route establishment starts after the attacker captures approximately 40% of all nodes in the network, i.e., when $\alpha \geq 0.4$. Moreover, as expected, the attack probability $P$ should be larger for smaller $\alpha$ in order to increase the route discovery failure probability. However, as it will be seen later in this section, it is not possible to increase $P$ value without increasing the risk of being detected.

In the simulations, the attacker randomly selects and compromises nodes in the network. For some selected percentage of compromised nodes, the attack probability is gradually increased and the number of route requests and route replies are observed. The simulation results of the proposed attack scenarios are presented in the following.

Route disruption attack reduces the ratio of route reply messages to the total number of route request messages. This ratio can be used by a network-wide detection system in order to check an unusual behavior. Fig. 4 shows how this ratio decreases as attack probability $P$ increases for different percentages of compromised nodes in the network. It is assumed there is a route disruption detection mechanism that watches the number of route replies over number of route requests as an evidence of an attack and the threshold value for this ratio is set to 1. The maximum attack probabilities ($P$) for not being detected by the detection mechanisms are found from Fig. 4 for different percentages of compromised nodes in the network. These $P$ values are used to check the route discovery failure probability ($P_R$) using the curves in Fig. 3. This analysis shows that the failure probability $P_R$ is around 0.1. In other words, on the average only 10% of the routes are broken by the attacks above the reply/request threshold of 1. For larger thresholds, $P_R$ reduces significantly: e.g., for the threshold value of 2, $P_R$ is as low as 0.02.

It can be deduced from these results that a simple detection mechanism employed in an ad hoc network can detect route disruption attacks before the attack can make any damage to the network.
As described in attack model, attack can be applied with a probability of 1 if there is no mechanism that detects routing disruption attacks. In such a case, the attack becomes effective ($P_R$ gets larger beyond 0.2) after approximately 30% of nodes in the network are compromised as shown in Fig. 3.

As an extreme case of analysis in the simulation study, in Fig. 5, a situation is considered where all the nodes are compromised. It is observed that even if all the nodes in the network are compromised, the number of route replies over number of route requests is still above the threshold value of 1 up to $P=0.2$. For this case, the route failure probability $P_R$ can be calculated using (3) as 0.04, i.e. 4% of the routes are broken.

The above analysis has an important performance implication, which is also valid when there is no attack on the network. It shows that some of route replies are redundant and an optimization may be possible on the number of route request re-broadcasts. If DSR is modified in such a way that the legitimate nodes re-broadcast the route requests with a probability of $P$, which should be engineered carefully, route discovery success ratio will still be acceptable and there will be a decrease in number of routing packets that are flooded to the network. Actually there is a threshold point for $P$ where the loss of routes starts to increase very fast.

![Simulation results of the change of reply/request ratio with respect to attack probability for different percentages of compromised nodes](image1)

**Figure 4.** Simulation results of the change of reply/request ratio with respect to attack probability for different percentages of compromised nodes

![Simulation results of the change of reply/request ratio with respect to attack probability when all nodes are compromised](image2)

**Figure 5.** Simulation results of the change of reply/request ratio with respect to attack probability when all nodes are compromised

**VII. CONCLUSIONS**

In this paper, a probabilistic attack model is proposed on DSR protocol and analyzed the effects of this model on route discovery success. In the attack model, it is assumed that attackers capture nodes and prevent re-broadcasting of route request messages. Even if the routing is secured using some cryptographic techniques, such a source-based disruption attack cannot be avoided. However, it can be detected by checking the route reply/route request ratio. In order not to get detected, attackers perform their attack in a probabilistic way.

Simulations have been done for different attack probabilities and different number of compromised nodes (attackers) in the network. The results for the example networks that we have analyzed show that such a probabilistic route disruption attack can be harmful by breaking approximately only 10% of the routes before getting detected. However, if there is no such detection mechanism, in which case the attack probability can be high and the attack may be very harmful. As a side result, the analysis of the attack model also showed that when all the nodes in the network are compromised, route discovery is not much disrupted till the attack probability $P$ reaches a certain value. This observation gives an idea that if the legitimate nodes suppress re-broadcasting route requests, DSR protocol performance can be improved to a large extent.

**REFERENCES**


