A Probabilistic Routing Disruption Attack on DSR and Its Analysis

Özleyiş Ocakoğlu, Burak Bayoğlu, Albert Levi, Özgür Erçetin and Erkay Savaş
Sabancı University, Faculty of Engineering and Natural Sciences,
Orhanlı, Tuzla TR-34956
Istanbul TURKEY
{ozleyiso, burakb}@su.sabanciuniv.edu
{levi, oercetin, erkays}@sabanciuniv.edu

Abstract — **In this paper, we propose an attack model against DSR ad hoc network routing protocol and analyze the effects of this attack model on DSR route discovery mechanism. The analysis of the attack model includes a probabilistic formulation to estimate route discovery failure. Simulations are performed to complement the analytic model. Results show that this attack can be kept in control with minimal harm on the network, provided that there is a detection mechanism; otherwise, with the increasing rate of compromised nodes, the harm on network tends to increase. As an interesting side result, our analysis also shows that our attack model can also be used to improve the performance DSR route discovery mechanism.**

Index Term s — **Ad Hoc Network Security, DSR, Route Disruption, Route Discovery.**

I. INTRODUCTION

Mobile Ad Hoc Networks (MANET) is an evolving research area with its applications in infrastructureless domains ranging from battlefields, disaster recovery to virtual classrooms. The infrastructureless nature of MANET implies that each node operates not only as a host, but also as a router. Thus, each node routes packets coming from other nodes towards their destination. There are several ad hoc routing protocols proposed in the literature [1, 3, 4, 5], but they do not consider security issues. Thus, they inherently have several vulnerabilities and exploits that may disrupt ad hoc routing. Such vulnerabilities have been demonstrated in [2, 6].

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, we focus on a routing disruption attack in DSR, in which attacker nodes do not re-broadcast route request packets and do not send cached replies with a probability *P*. This affects the route discovery mechanism depending on the number of attackers in the network and the attack probability *P*. The rationale of the attacker behind applying the attack in a probabilistic way, but not by dropping all route request packets, is to be resistant against any possible behavioral attack detection mechanism in the network.

We primarily investigated the feasibility of the attack from the attackers' point of view and the importance of the detection mechanism to reduce the negative effects of the attack using a mix of analytical and simulation studies. As a result, we have seen that it is possible to diminish the negative effects of the attack on the route discovery success by employing a detection mechanism.

As a secondary result, while investigating the effects of our attack model to the DSR protocol, we realize that the route discovery success ratio does not degrade significantly until a certain attack probability. This gave us the 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 to the network.

The rest of the paper is organized as follows: In Section II, we give an overview of DSR protocol. Section III summarizes the routing disruption attacks against DSR. In this section we also give our attack model and its characteristics. Section IV presents an analytical model for our attack that is used in numerical analysis in Section V. Simulation results that investigate the effects of the attack model from both attacker and defender points of view are also discussed in Section V. Section VI gives an overview of performance improvement research in ad hoc networks and the implication of the proposed model in this avenue.

II. OVERVIEW OF DYNAMIC SOURCE ROUTING (DSR)

DSR Protocol is a routing protocol designed for mobile wireless ad hoc networks by Johnson, Maltz, and Hu [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 learned 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 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, by 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, then 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.

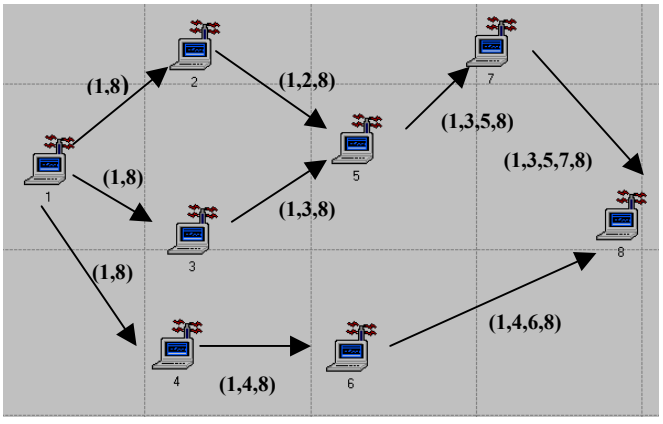

Fig. 1. Route discovery example

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 address to the request packet and rebroadcast the request. Since nodes 2, 3 and 4 have just processed the request, they will discard the re-transmitted requests 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; add its address and re-broadcasts. On the other hand, node 6 receives the request from node 4 and re-broadcasts 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 acknowledgement mechanism in DSR. Every node ensures that data flows from one node to the next one by requesting acknowledgements. A node not receiving acknowledgement will transmit acknowledgement requests for a certain period of time. If no acknowledgement 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. Routing Disruption Attacks Against 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 [2].

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 [6], increase routing traffic or end-to-end latency, and even partition the network.

A. Attack Model

As briefly overviewed in Section II, nodes process route requests by sending back cached route replies or by re-broadcasting route requests in DSR route discovery phase whereas dropping some redundant ones. A possible attack against Route Discovery mechanism of DSR is to capture a node and not process route request

packets. In the rest of the paper, we focus on a variation of this type of attack.

Our attack scenario is as follows:

1) When an attacker who has previously captured a normal node receives a route request packet, it checks if there exists a route to the destination in the route cache.
2) 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.
3) If there is no cached route to the destination, in contrast to normal nodes, attacker does not re-broadcast this route request with the same probability P. In other words, the attacker re-broadcasts 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 highest 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 be resistant against any detection mechanism employed in the ad hoc network. If there is a mechanism that detects routing disruption attacks, attacker will not be detected until compromising a certain number of nodes and/or increasing the attack probability. These threshold values are analyzed in Section V. The mechanisms that can be used to detect attackers are out of scope of this paper.

Such an attack appears quite plausible in hostile environments. The attack model assumes that attackers capture legitimate and operational nodes such that the attacker is able to access all of the facilities of this node with its normal user's rights and privileges. Even if the route discovery is secured with encryption and authentication measures, the attacker may still physically capture the node and prevent route reply and re-broadcasting the route requests by controlling the node. An encryption or authentication measure does not prevent this type of an attack.

The proposed attack that limits re-broadcasting the route request packets does not always prevent route discovery. 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 certain number of nodes is 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 the next two sections.

IV. Analytical Model

We propose a probabilistic model to analyze the effects of the attack on route discovery mechanism. The parameters that we use in our model are given below:

N Average number of nodes per route

R Average number of paths returned for the same route request and for the source-destination pair

P Probability of not re-broadcasting, i.e., attack probability

α Ratio of compromised nodes over number of all nodes, 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* of the nodes on a path with average length N will re-broadcast the route request or return the route reply from their cache is:

$$(\alpha \cdot (1-P) + 1 - \alpha)^N \qquad (1)$$

The above formula 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 as follows.

$$P_0 = 1 - (\alpha \cdot (1-P) + 1 - \alpha)^N \qquad (2)$$

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, we may assume 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.

$$P_R = (1 - (\alpha \cdot (1-P) + 1 - \alpha)^N)^R \qquad (3)$$

By estimating the values of N and R, the attackers can utilize (3) to find out the attack probability (P) values for aimed route discovery failure probabilities. Such an analysis is given in the next section.

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

V. Experimental and Numerical Results

Simulations are performed in OpNet Modeler 10.0 environment. The example network consists of 100 static nodes. The routing algorithm used is DSR and nodes are running multiple FTP sessions from an FTP server.

When there are no attackers in the system, Fig. 2 shows that number of route replies is, on the average, six times more than the number of route requests. Using this information, R value (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. We use these values for the analysis of the analytical model given in Section IV.

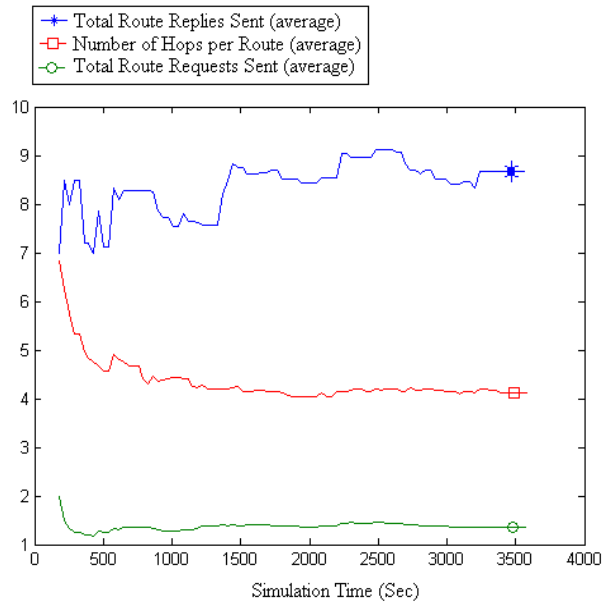

Fig. 2. Simulation of the example network with no attackers

The change of P_R with respect to P for the simulated network described above is depicted in Fig. 3 for different α values. (3) is used for this analysis. For the simulated network, P_R is very low for α = 0.1 and α = 0.2, even if the attack probability P is 1. Significant damage on the route establishment starts after the attackers capture approximately 40% of all nodes, i.e., when α >= 0.4. Moreover, as expected, the attack probability P should be larger for smaller α in order to increase the route discovery failure probability. However, as we shall see later in this section, it is not possible to increase P value without taking the risk of being detected.

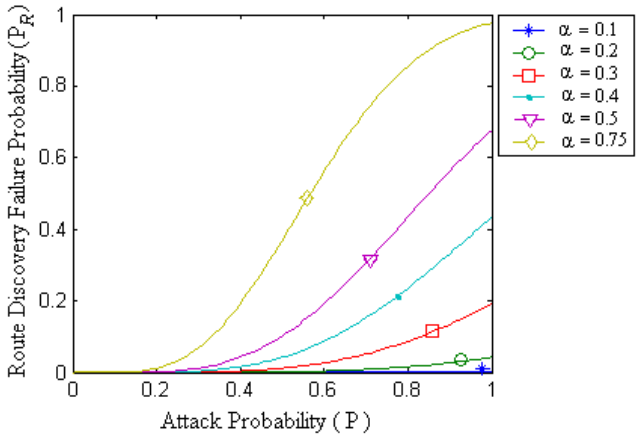

Fig. 3. The change of route discovery failure probability with respect to attack probability for different fractions of compromised nodes

In our simulations, attackers are randomly selected among the normal nodes. For the selected percentage of attacker nodes, we gradually increased the attack probability and observed the number of route requests and route replies. Below are the simulation results of the proposed attack scenarios.

Route disruption attack reduces the ratio of route reply messages over the number of route requests. This ratio can be used by a network-wide detection system in order to check an unusual behavior. Thus, we analyzed this ratio in our simulations. Fig. 4 shows how this ratio decreases as attack probability P increases for different fractions of compromised nodes. We assume that there exists 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. Then, the maximum attack probabilities (P) for not being detected by the detection mechanism are found out from Fig. 4 for different compromised node ratios. 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.

We can deduce from these results that a simple detection mechanism employed in an ad hoc network

can detect route disruption attacks before the attack gets worse.

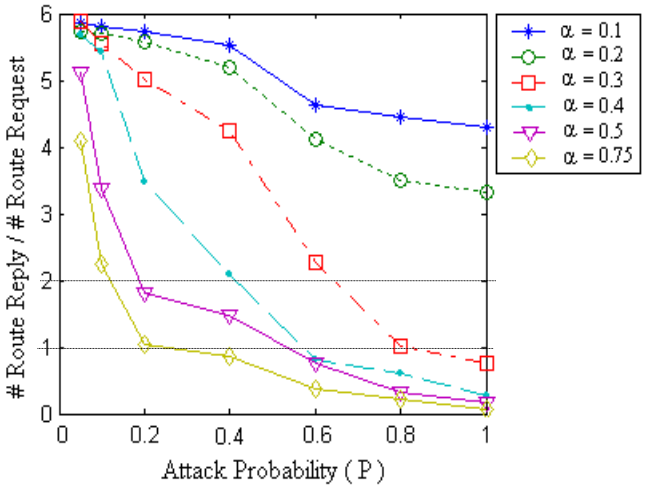

Fig. 4. Simulation results of the change of reply/request ratio with respect to attack probability for different fractions of compromised nodes

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 are compromised as shown in Fig. 3.

As an extreme case analysis in our simulation study, in Fig. 5, we considered the situation where all nodes are compromised. Fig. 5 shows that even if all of the nodes 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. only 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. A similar conclusion has been reached using percolation theory in [9].

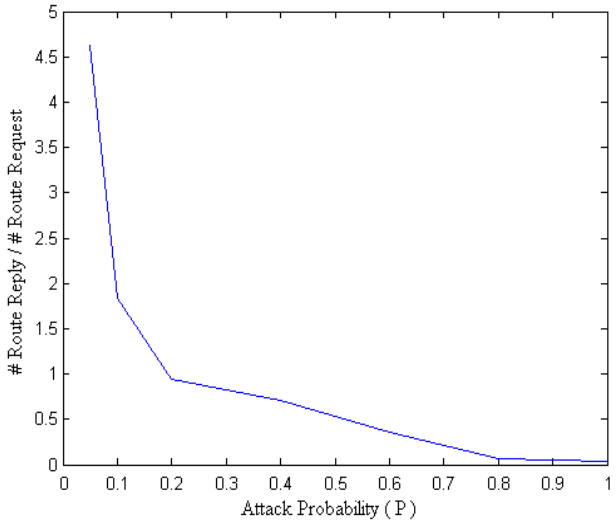

Fig. 5. Simulation results of the change of reply/request ratio with respect to attack probability when all nodes are compromised

VI. Related Work and Discussion on Performance Improvement Aspects

The main idea behind performance improvements in ad hoc networks is that ad hoc network clients are strictly restricted of system resources, especially computational time and energy. Any improvement that decreases the overhead for the same amount of work will help the ad hoc clients utilize system resources much more efficiently. Santi and Blough have showed that reducing the transmission range of the ad hoc client saves energy while making the network less connected [12].

If a node has the path to the requested node in its route cache, it will return a route reply and normally will not re-broadcast. This obviously shows the importance of route cache validity and having up-to-date information. In [13], He et al. proposed that the use of Active Packets which visit all the nodes to learn the network topology and maintain route caches is useful for decreasing the number of route request re-broadcasts. In [14], Wu proposes a new approach to decrease the number of route discovery packets. The paper defines an extension to dynamic source routing algorithm with no or little overhead to the normal route discovery. The idea is to find two alternative paths to a destination, one is master and the other is backup. Backup route decreases the number of route request floods sent to the network.

In [7], redundancy caused by the flooding type of broadcast is analyzed and various types of broadcasting mechanisms are proposed in order to reduce redundant transmissions. Later, Williams and Camp discussed

different kinds of broadcasting mechanisms, and proposed a probabilistic broadcasting mechanism in [8]. They showed in [7, 8] that probabilistic broadcasting performs well when the distribution of nodes in the network is dense.

Sason et al. used the phase transition concept from percolation theory to estimate the probability of broadcasting [9]. Phase transition is a kind of threshold point where the system behavior changes suddenly and after this threshold the system tends to have a global behavior [10]. Percolation theory is widely used in many previous researches [11].

Decreasing the number of packets that are re-broadcast means decreasing the number of packets that a client processes and also decreasing the number of redundant packets in the network. In DSR, although it is possible to end up with route discovery failures to some extent, not re-broadcasting route request packets with certain probability can be considered as a performance improvement technique. In this context, although the details of such an analysis are left as future work, the attack model and analysis that we proposed in this paper for the case where $\alpha = 1$ can be considered as a probabilistic approach for performance improvement in DSR. Preliminary results that we have reached in this study show that for the example network that we analyzed, it is possible to reduce the reply/request ratio to 1 with a cost of 4% route failures, and to 2 with a cost of 0.16% route failures.

VII. CONCLUSIONS

In this paper we proposed a probabilistic attack model against DSR ad hoc network routing protocol and analyzed the effects of this attack model on route discovery success. In our attack model, we assume 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. We have performed simulations for different attack probabilities and different number of compromised nodes (attackers).

The results for the example networks that we 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 employed in the system, in which case the attack probability can be simply 1, then the attack may become so harmful depending on the fraction of the compromised nodes. From this we conclude that a detection and reaction mechanism should be employed against route disruption attacks, but the details of these mechanisms are not in the scope of this paper.

As a side result, our analysis also showed that when all the nodes are compromised in the network, route discovery is not so disrupted up to a certain attack probability, P, value. This is due to redundant route replies for a route request. This observation gave us the idea that if the legitimate nodes suppress re-broadcasting route requests, DSR protocol performance could be improved. Such a change of re-broadcast mechanism in DSR route discovery phase comes with some drawbacks and also advantages, so there is a tradeoff here. The most important advantage is the increase in network utilization by decreasing the overhead of redundant broadcasts. However, one should note that, the route discovery time increases and there is a small probability of not being connected for some nodes.

REFERENCES

[1] David B. Johnson, David A. Maltz, and Josh Broch. *DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks*. in Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.

[2] Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer. A secure routing protocol for ad hoc networks. Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, November 2002, pp. 78-90.

[3] Charles E. Perkins and Elizabeth M. Royer. Ad hoc On-Demand Distance Vector Routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.

[4] Charles E. Perkins and Elizabeth M. Royer. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. Computer Communications Review, Oct. 1994, pp. 234-244.

[5] E.M. Belding-Royer and C. K. Toh. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications Magazine, April 1999, pp. 46-55.

[6] Chris Karlof and David Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasure. Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

[7] S. Ni, Y. Tseng, Y. Chen, and J. Sheu. The broadcast storm problem in a mobile ad hoc network. Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), 1999, pp. 151–162.

[8] T. Camp and B. Williams. Comparison of broadcasting techniques for mobile ad hoc networks. Proceedings of The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC 2002), Lausanne, Switzerland, Jun 2002, pp. 194-205.

[9] Y. Sasson, D. Cavin, and A. Schiper, Probabilistic broadcast for flooding in wireless mobile ad hoc networks, in Proceedings of IEEE Wireless Communications and Networking Conference (WCNC 2003), New Orleans, LA, Mar.2003.

[10] B. Krishnamachari, S.B. Wicker, and R. Bejar. Phase transition phenomena in wireless ad-hoc networks. Proceedings of the Symposium on Ad-Hoc Wireless Networks (GlobeCom2001), San Antonio, Texas, Nov. 2001.

[11] P. T. Olivier Dousse and M. Hasler, Connectivity in ad-hoc and hybrid networks, Proceedings of IEEE Infocom, New York, June 2002.

[12] Paolo Santi, Douglas M. Blough, The Critical Transmitting Range for Connectivity in Sparse Wireless Ad Hoc Networks, IEEE Transactions on Mobile Computing, v.2 n.1, January 2003, pp. 25-39.

[13] He, Y., Raghavendra, C., Berson, S., Braden, R. Active Packets Improve Dynamic Source Routing for Ad-hoc Networks. Proceedings of IEEE OpenArch 2002, Short Paper Session, June 2002.

[14] Jie Wu, An Extended Dynamic Source Routing Scheme in Ad Hoc Wireless Networks. Telecommunication Systems, a special issue on Wireless Networks and Mobile Computing, 22, 1-4, 2003, pp. 61-75.