# Analyzing the Impact of Misbehaving Nodes in Ad Hoc Routing *

Luiz Gustavo S. Rocha  Luís Henrique M. K. Costa  Otto Carlos M. B. Duarte

Grupo de Teleinformática e Automação
COPPE/EE – Programa de Engenharia Elétrica
Universidade Federal do Rio de Janeiro
http://www.gta.ufrj.br/
{lgrocha,luish,otto}@gta.ufrj.br

**Abstract**

Routing is the key issue for ad hoc networks due to the wireless medium, absence of infra-structure and distributed operation. In ad hoc networks, every node acts as a router. Hence, securing the routing mechanism is a critical issue. This paper analyzes attacks that exploit the vulnerabilities of the ad hoc routing mechanisms. The attacks are based on the malicious behavior of some network nodes, disturbing the forwarding of control messages. AODV is the routing protocol chosen for study. AODV is a reactive protocol, specific for ad hoc networks, whose routes are setup on demand. Therefore, the malicious behavior of some nodes may affect the whole network performance. The paper shows the effect of different attacks based on simulation results of the action of malicious nodes. We identify the most effective attacks in terms of network performance degradation using the total data packet delivery rate as metric.

***Key-words:*** mobile ad hoc networks, routing, security.

## 1 Introduction

Wireless mobile ad hoc networks (MANETs) are self-organizing networks where each node plays a role in the routing system. Therefore, routing is the most sensitive mechanism of ad hoc networks, since all services operation depends on its performance. Due to the importance of the routing mechanism , most of the research on security on wireless ad hoc networks focuses on secure routing [1, 2, 3]. Security is a key feature that can boost the widespread use of this communication technology, including most sensitive security application in hostile environment. Nevertheless security requirements are difficult to achieve due to the specific characteristics of ad hoc networks as bandwidth-constrained wireless links, limited process power and battery life of mobile devices, unpredictable mobility of nodes and network membership variability [4, 5, 6].

This work analyzes attacks against the routing system, that are based on the misbehavior of nodes with respect to routing messages. It evaluates the impact of such attacks in a typical environment application of this communication technology regarding number of compromised nodes and mobility degree. Its important to understand how the attacks degrade the network performance, helping to foresee solutions to the mistreatment of routing messages by compromised nodes.

This paper is organized as follows. Section 2 describes the main aspects of ad hoc routing, secure routing and the choice of routing protocol for the simulation. Section 3 describes the simulation environment, the attack models and the performance analysis. Section 4 concludes the paper.

* This work is supported by CAPES, CNPq, FAPERJ, COFECUB and FUJB.

# 2 Ad hoc Routing

Routing is the mechanism responsible for keeping the network connectivity. Ad hoc routing protocols have to cope with the special requirements of the wireless medium, node mobility and structureless networks. In such networks, every node act as a router, and the routing management and operation are completely distributed [7].

With respect to the routing operation model we are interested in two categories of protocols, the *table-driven* protocols and, mainly, the *on-demand* protocols [8].

The table-driven model maintains tables in each node with updated routing information to every other node in the network, it operates pro-actively. To keep a consistent network view, messages are periodically propagated throughout the network. This avoids errors from changes in the network topology [7, 8]. This is the routing model used in conventional wired networks, which was adapted to the wireless networks.

The flip-side approach, on-demand, also known as source-initiated model, creates routes only when they are needed. The route discovery process is initiated when a source node requests a route to a destination node. A maintenance procedure keeps the established route until either it is no longer needed or the destination becomes unreachable [7, 8].

Both routing protocol models have to provide connectivity with the lowest overhead and bandwidth consumption possible, and to forward packets efficiently to support delay sensitive applications.

The on-demand approach, also know as reactive, is the type of routing protocol specially designed for the wireless mobile ad hoc networks. Therefore, it is important to investigate the behavior of reactive routing protocols under attacks.

The routing protocol selected for study is AODV (Ad Hoc On-Demand Distance Vector) [8]. AODV is a source-initiated routing protocol chosen for its widespread use and presence in several other studies [2, 3, 9]. Currently, AODV is under standardization [10] in the MANET (Mobile Ad hoc NETwork) working group of the IETF (Internet Engineering Task Force). Section 2.2 gives more details about the AODV protocol.

## 2.1 Secure Routing

Mobile ad hoc networks are more prone to security threats than conventional hardwired networks due to its kind of operation. The security mechanisms and the basic operation mechanisms may have vulnerabilities. Eavesdropping, spoofing, tunneling, man-in-the-middle, and denial-of-service attacks must be carefully considered for new security implementations, specially given the wireless nature of MANETs. Routing is a vulnerable point of the basic operation mechanisms because if routing is misdirected the entire network can be paralyzed. Thus, secure operation of the routing protocol plays an important role for MANETs, envisioning operation in an open, collaborative, and harsh environment [2, 7].

Attacks against the network basically aim the discovery of previously inaccessible information and the denial of network services. Such attacks can be categorized into *passive* and *active*, depending on the behavior of the compromised node, and into *internal* and *external*, depending on the membership of the compromised node [5]. Active attacks generate traffic in the targeted network, whereas passive attacks do not. Internal attacks are generated by nodes inside the network and external attacks by nodes outside it. Passive external attacks do not disrupt the network operation, but attempt to listen the network traffic, including routing traffic, to obtain some valuable information. This kind of attack is difficult to detect, because the listener device is not a network member node. The most severe of the attacks is the internal active one, where a hijacked node carries through an attack classified as protected, since it is an authenticated/authorized node of the network. It is also possible that compromised nodes operate in group. They can insert, modify and delete messages, including the routing messages [1, 2].

The threat of denial of service or performance degradation based on the mistreatment of routing messages is an internal passive attack and constitutes a notable vulnerability in a distributed system, such as ad hoc networks. This mistreatment of routing messages can be originated in unintentional erroneous operation [2] or in malicious actions of network elements [4, 6].

The basic ideas of security mechanisms for ad hoc networks descend from the traditional approach of the security problems of conventional communication networks. Therefore, ideas like authentication protocols, redundant transmission, digital signatures and cryptography keys still play an important role [3, 11].

## 2.2 AODV Routing Protocol

The Ad hoc On-demand Distance Vector (AODV) [10] routing protocol is an improvement on the Destination-Sequenced Distance Vector (DSDV) [12] routing protocol. AODV creates routes on demand, trying to minimize the number of control messages. Given that nodes that are not in the selected path do not maintain routing informations or exchange routing table informations, and that the process is source initiated, AODV is classified as a *pure* on-demand routing protocol (except when using *hello* messages).

The path discovery process starts when a source node desires to send a message to a destination node and does not have a valid route. The source node broadcasts a *route request packet* (RREQ) to its neighbor nodes, which then forward the request to their neighbor nodes, and so on. The process continues until either the destination node, or an intermediate node with an updated (fresh enough) route to the destination, is reached by this request. Then, the node responds with an unicast *route reply packet* (RREP) back to the neighbor from which it first received the RREQ. The AODV protocol only supports symmetric links. The reply packets are routed back along the reverse path established by the request packets. The reply packets that travel along the intermediate nodes setup forwarding entries in the routing tables. These table entries point to the node from which the RREP was received. There is a timer associated with each route entry. The entries expire if not used by data packets. Destination sequence numbers are used by AODV to ensure loop-free routes and up to date routing information.

With the mobility and radio interferences, links in the network can go down and a route repair procedure may be necessary. If a node moves out of the radio range of its neighbor, the upstream neighbor propagates a link failure notification (*routing error packet* - RERR) to each of its upstream neighbors to inform the failure of part of the route. The failure notification is propagated until the source node is reached. When the source node is reached by the routing error packet it initiates a new path discovery process.

Connectivity information can be obtained using *hello* messages. Hello messages are routing reply packets with TTL 1, which are periodically broadcasted by a node to inform its existence to its neighbors. The use of hello is part of the protocol specification, but it can be suppressed if the MAC layer provides this functionality. More details about the AODV routing protocol can be found in [3], [9], [8] , and [10].

# 3 Performance Evaluation of Security

## 3.1 Modeling and Simulation

The attacks against ad hoc routing can be implemented simply by the malicious behavior of nodes in relation to the routing messages and have the objective to degrade, or even to avoid, the delivery of data packets. The attack is based on the non-collaborative action of malicious nodes with respect to AODV messages. To simulate such behavior new routing agents were created based on the modification of the original AODV routing agents. These new agents have special characteristics in relation to each one of the three types of AODV routing messages.

The attack against *route error* messages (ERR attack) is implemented by the MAL-ERR agent. The agent identifies the reception of RERR packets and do not transmit these packets to predecessor nodes. The mistreatment of received *route reply* messages is implemented by the MAL-REP agent (REP attack). The REP attack prevents the transmission of RREP packets that use the node as route. Nevertheless, in case of reception, the node uses the information of these packets for proper benefit, updating its routes. The attack against *route request* messages (REQ attack) is accomplished by the MAL-REQ agent, which does not propagate and answer route requests, only in behalf of itself, thus acting non-collaboratively also.

The REQ, REP and ERR attacks are executed separately. In each simulation a certain number of nodes is created with one of the modified agents. The objective is to evaluate the effectiveness of the attacks regarding the number of malicious nodes and the degree of node mobility. The metric used is the total delivery rate of data packets in the network. This metric measures the effectiveness of the implemented attacks.

We used the *ns-2* [13] simulator version *2.1b9a* together with the extension of mobility and multihop wireless networks developed by the Monarch Project [14]. This extension to *ns-2* models the IEEE 802.11 standard, implementing physical, medium access control and data link layers and the DCF (Distributed Coordination Function) operation. It also implements the AODV routing protocol, among others, and provides tools for mobility scenarios and traffic pattern generation.

Our simulation scenario uses a network composed by 60 mobile nodes. The model of mobility is *random waypoint* [14]. Nodes move on a rectangular area of 1200m x 500m with maximum speed of 20m/s and varying pause time. The total simulation time is 600s. The radio range of the devices is 250m. The traffic is CBR (Constant Bit Rate) formed by 512 bytes packets with 4 packets per second rate. The number of source/destination pairs is 30. The network operates at 11Mb/s. This scenario is similar to the one used in [9] for comparison of routing performance.

### 3.2 Results and Analysis

There are three graphs (Figures 1, 2, and 3) that present the results of simulations for different mobility conditions. Each of them presents three curves referring to the three types of attack (REQ, REP and ERR). The abscissas axis (x) is the percentage of compromised nodes in the attack, the ordinate axis (y) is the percentage of delivered data packets. Each mobility scenario has a different pause time (0, 300 and 600 seconds) and the total simulation time is 600s. A confidence interval of 95% was used for the accomplishment of the simulations and it is represented by vertical error bars in the graphs.

The first general remark is that the mobility degree changes the behavior of the three attacks comparing the three graphs. The first point of the curves (x = 0) corresponds to the situation where there are no malicious nodes and therefore no attacks. Thus, all curves in the three graphs coincide, as expected. The value of these points, around 99% of packet delivery, indicates a very low network load. Links operate at the nominal rate of 11Mb/s and the traffic of useful data consumes only 16Kb/s for each source node and 500Kb/s for the maximum load of the whole network.

In a high mobility scenario, the connectivity between nodes has a lot of variation. It means that source and destination are sometimes in direct contact (one hop) and are sometimes connected by multiple hops. This environment demands more effort of the routing mechanism. The routing protocol must execute several procedures of route discovery and route maintenance. The high mobility environment is represented in the Figure 1. Observe that the ERR attack is very harmful, being able to lower the delivery rate down to 60%. This is due to the huge number of route errors that occur in an environment of high mobility. With the ERR attack, the RERR messages may not arrive at the source nodes. The REP attack is harmless because the high mobility environment leads to intense route variation, then, anyway, a RREP packet installs routes that will not be valid for a long time. The REQ attack starts to be effective when more than 70% of nodes are compromised and block the propagation of route requests. With fewer malicious nodes in action the scenario of high mobility reduces the influence of these nodes due to the possibilities of establishing routes by safe nodes. If more than 80% of the nodes are compromised in this attack, the establishment of multihop routes becomes very difficult. Only the destination nodes that are in the direct reach of sources nodes (corresponding one hop routes) remain connected. This leads to the delivery rates as low as 35%.

In an environment without mobility (represented in the Figure 3), everything depends on initial position of the nodes in each simulation scenario. As there is no movement, the influence of an ERR attack is null because of the absence of route failure notifications. A given node will always be in the range of some nodes and it will never be reachable by other nodes. The network connectivity does not change. As a consequence, the multihop routes are not modified during the simulation. Only when more than 50% of the network nodes are compromised in the attack, it is possible to observe an influence of the REP and REQ attacks. When more than the half of nodes is compromised, the effectiveness of the REQ attack is larger than the REP attack. The REQ attack can low the delivery rate down to 20%. In this situation the establishment of routes is difficult due to the behavior of more than the half of the network with respect to route requests and to the static state of nodes during all simulation time. In the REP attack the worst situation leads to 80% of delivery rate, because there is a probability that source and destination are directly reachable. Therefore, with exactly 100% of malicious nodes, routes with only one hop are not affected by the attack, explaining its low effectiveness.

Note that the curves in Figure 2 are a transition from Figure 1 to 3. It corresponds to an environment where, in

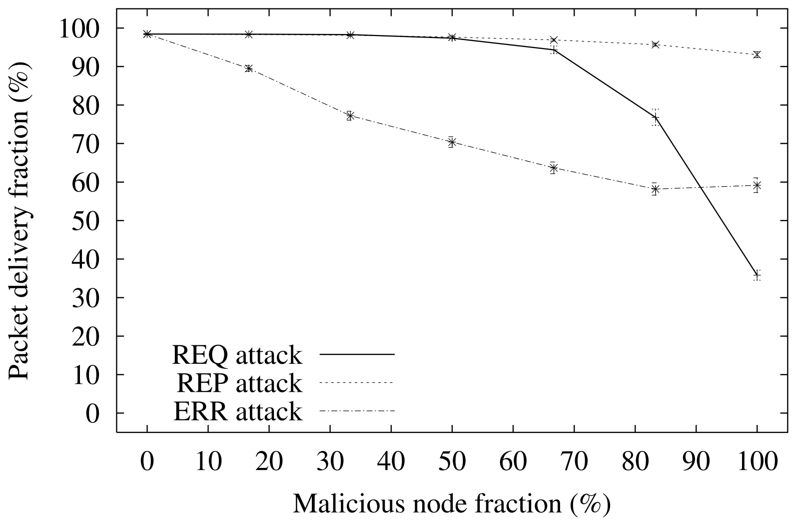


Figure 1: Performance degradation due to the attacks against routing, without pause time.

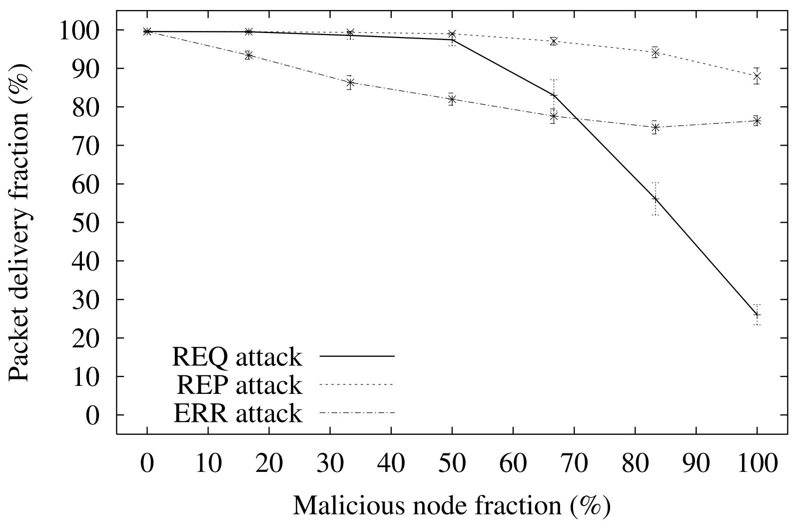


Figure 2: Performance degradation due to the attacks against routing, pause time 300s.

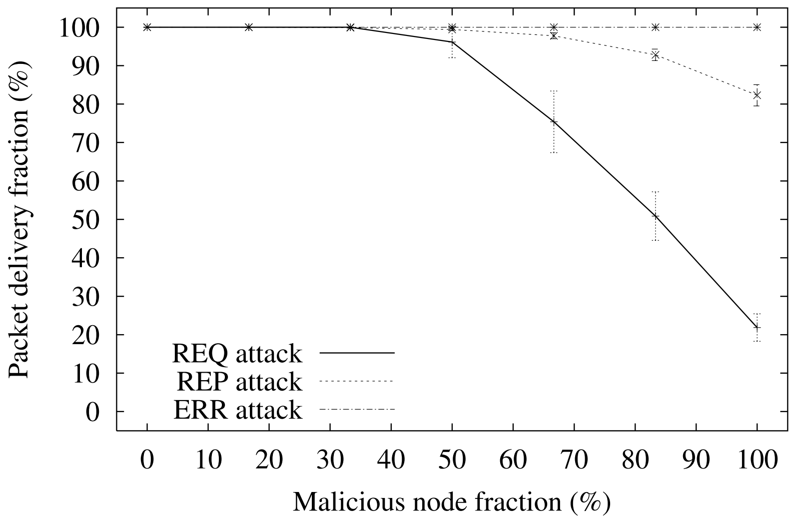


Figure 3: Performance degradation due to the attacks against routing, without movement.

average, nodes move during half of the simulation time and in the other half of the time they are static. This figure confirms the results in the extremities conditions, i.e. total mobility and no mobility.

In summary, the attack to the reply messages (REP) is the less sensitive to variations in the network mobility degree. The most sensitive attack to these variations is the error message (ERR) one. The most sensitive attack regarding the number of malicious nodes is the attack against the request messages (REQ), and the less sensitive is the attacks to the replies (REP). Thus, in an application environment of intense mobility the attack against the error messages is the most effective. On the other hand, in an environment of low mobility degree the attack against the route request is the most effective. Regarding the density of nodes involved in the attack, in all cases, the larger is the amount of compromised nodes, the more efficient is the attack.

The routing mechanism, operating with the AODV protocol, demands a assistant mechanism to prevent the misbehaving nodes from degrading the network performance, specially the mistreatment of the route error messages in a high mobility environment and of route request messages in a low mobility environment. This assistant mechanism could use ideas, such as the *watchdog* and the *pathrater* mechanisms, exposed in [1] and adapt the proposed mechanisms to the AODV protocol operation. The version of the AODV proposed in [3] incorporates security enhancements but do not solve this routing security flaw. These enhancements are based on digital certification and cryptography and does not address non-collaborative node behavior. To mitigate this significant vulnerability the routing assistant mechanism must first identify these misbehaving nodes and afterwards help the AODV protocol to avoid these nodes. Even if the routing overhead can increase with this assistant mechanism, the network goodput should increase in the eventuality of attacks.

# 4 Conclusion

The ad hoc networks constitute an area of great challenges when it refers to the security aspects. The basic mechanisms of network operation still present vulnerabilities in its current implementations. In special, the routing mechanism deserves more attention from the research community due to the possibilities of attacks that it offers, as an example, a DoS (Denial of Service attack). Such attacks aim to avoid or to degrade the network operation through the malicious and non-cooperative actions of some nodes. The targets of these actions are the routing control messages exchanged between all nodes in an ad hoc network.

In this paper we evaluated the impact of the malicious action of compromised nodes in an ad hoc network based on the study of the AODV routing protocol. The metric used was the total data packet delivery rate, which variated in function of the mobility, the type of attack, and the density of compromised nodes.

The results obtained point the necessity of mechanisms capable of avoiding or mitigating the non-cooperative behavior of nodes. The effectiveness of the different attacks vary in function of the mobility degree and the density of nodes compromised in the attack. Therefore, certain types of messages must have protection priority. For each environment a type of attack is more harmful. The routing error messages must receive immunization priority in scenarios of high mobility degree, although in scenarios with low mobility degree the route request messages must be prioritized against mistreatment.

Together with the routing protocol, an additional security mechanism must operate to help the main routing mechanism to identify and avoid the compromised nodes. The current security enhancements of the AODV protocol, based on digital certification and cryptography, do not address this type of threat. The trade-off between the overhead of routing control messages and the goodput of the network must be investigated to foresee the best operation point.

Our future work will consider an inquiry of other types of attacks and mechanisms capable to protect against such attacks. Such mechanisms must be compatible with the restrictions imposed by ad hoc networks, specially the scarce bandwidth and energy of the mobile devices, and still do not harm the network performance.

# References


[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *ACM International Conference on Mobile Computing and Networking - MobiCom*, 2000.

[2] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 70–75, Oct. 2002.

[3] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the ACM workshop on Wireless Security - WiSe*. ACM Press, Sept. 2002.

[4] J. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks," in *ACM International Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc*, 2001.

[5] V. Karpijoki, "Security in ad hoc networks," Department of Computer Science, Helsinki University of Technology, Tech. Rep., 2001.

[6] A. Vanhala, "Security in ad hoc networks," Department of Computer Science, University of Helsinki, Tech. Rep., 2000.

[7] S. Corson and J. Macker, *Mobile Ad hoc Networking (MANET) - Routing Protocol Performance Issues and Evaluation Considerations*, Jan. 1999, http://www.ietf.org/rfc/rfc2501.txt.

[8] E. M. Royer and C. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, no. 2, pp. 46–55, Apr. 1999.

[9] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Personal Communications*, vol. 8, no. 1, pp. 16–28, Feb. 2001.

[10] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, *Ad Hoc On-Demand Distance Vector (AODV) Routing*, Feb. 2003, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-13.txt.

[11] Z. J. Haas and L. Zhou, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[12] C. E. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers,” in *ACM Conference of the Special Interest Group on Data Communication - SIGCOMM*, 1994.

[13] K. Fall and K. Varadhan, *ns Notes and Documentation*, UC Berkeley, LBL, USC/ISI, and Xerox PARC (The VINT Project), Apr. 2002, http://www.isi.edu/nsnam/ns/ns-documentation.html.

[14] Monarch Project, *The Rice Monarch Project – Wireless and Mobility Extensions to ns-2*, Nov. 2000, http://www.monarch.cs.rice.edu/cmu-ns.html.