A Simulation Analysis of Routing Misbehaviour in Mobile Ad Hoc Networks

Abdelaziz Babakhouya, Yacine Challal, Abdelmadjid Bouabdallah

A Simulation Analysis of Routing Misbehaviour in Mobile Ad hoc Networks

Abdelaziz Babakhouya
CERIST Center of Research, Algiers, Algeria.
University of Béjaia, Algeria.
babakhouya@cerist.dz

Yacine Challal
Heudiasyc lab. UMR CNRS 6599
UTC,
Compiègne, France.
ychallal@ hds.utc.fr

Abdelmadjid Bouabdallah
Heudiasyc lab. UMR CNRS 6599
UTC,
Compiègne, France.
bouabdal@ hds.utc.fr

***Abstract*— Mobile Ad hoc Networks (MANETs) rely on the cooperation of all participating nodes to provide the fundamental operations such as routing and data forwarding. However, misbehaving nodes may not follow the cooperation paradigm and cause a serious affect on network performance. Nodes misbehave because they are malicious, selfish or malfunctioning. In this paper, we present a simulation study of the effects of misbehaving nodes on DSR routing protocol performances and discuss some countermeasures to mitigate misbehaving node effects.**

Keywords- MANET, Routing, Simulation, Selfish, Malicious, Attack, Security.

I. INTRODUCTION

A Mobile Ad hoc NETwork (MANET) is a collection of wireless mobile nodes which may form a temporary network, without the use of any fixed infrastructure or centralized administration [1]. Nodes rely on multi-hop routing protocols to forward data packets sent from a source node to a destination node which is out of its transmission range. Every node may function as both a data source and a router that forward data for other nodes.

Routing protocols are essential for a MANET in order to discover network topology and build routes, MANET routing protocols are designed to dynamically maintain routes between any pair of communicating nodes in spite of frequent topology changes caused by nodes' mobility. A lot of routing protocols have been proposed in the literature [2], including proactive, reactive, and hybrid solutions. Broch et al. [3] gives a simulation study of MANET routing protocols on different mobility and traffic scenarios. Djenouri et al. [4] have shown that reactive protocols are more adaptable to MANET environments than proactive protocols. Dynamic Source Routing (DSR) [5] is a reactive routing protocol which is largely adopted by IETF's MANET working group [6].

The problem of all the current ad hoc routing protocols is that they trust all nodes and assume that they behave properly; therefore they are vulnerable to attacks launched by misbehaving nodes. According to [7] nodes misbehave because they are *malfunctioning*, *selfish* or *malicious*. Malfunctioning nodes are simply suffering from hardware failure or software errors. Selfish nodes can agree to forward packets on behalf of other nodes but silently drop the packets in attempt to save their resources (energy and bandwidth). Malicious nodes may try to sabotage other nodes or even the whole network, for example one malicious node can advertise itself as having the shortest path to all nodes in the network then it can cause Denial of Service (DoS) by dropping all the received packets, in *Black hole attack*, or selectively dropping packets in *Gray hole attack*. Even more, malicious nodes can cause sever damage by collaborating in the attack, such as *wormhole attack*. Several ad hoc routing protocols attacks [8, 9, 10] have been discussed in the literature. However, as far as we can say, there is not a deep study of the impact of such attacks on the performance of routing protocols through simulations.

To provide network services under the presence of misbehaving nodes, it is necessary to consider "fault tolerance" as a main objective at the design level of routing protocols. To address this concern, several secure routing protocols have been proposed recently. Some of these protocols handle attacks by malicious nodes but not the selfish nodes and some handle selfish nodes but not malicious nodes. At the best of our knowledge, there is no solution that handles all misbehaving nodes actions. We think that it is necessary to provide a simulation study that measures the impact of misbehaving nodes in order to provide protocol designers with new guidelines that help in the design of fault / attack tolerant routing protocols for MANETs.

In this paper, we give a simulation study of misbehaving nodes impact on DSR [5] performance. First of all, we present an overview of DSR in section II. Then, in section III, we give details on our misbehaving nodes model that include both selfish and malicious nodes at routing level. In section IV, we measure, through different simulation scenarios, DSR performance in presence of each type of misbehaving nodes. We end up our paper by some countermeasures to secure or mitigate misbehaving nodes impact.

II. OVERVIEW OF DSR

DSR [5] is an on-demand routing protocol which is based on source route approach. In this approach, each packet carry in its header the source route which contains the complete, ordered list of nodes through which the packet must pass.

The DSR protocol consists of two mechanisms: Route Discovery and Route Maintenance. Route Discovery is the mechanism by which a node ***S*** wishing to send a packet to a destination ***D*** obtains a source route to ***D***. To perform a Route Discovery, the source node ***S*** broadcasts a ROUTE REQUEST

(RREQ) packet that is flooded through the network in a controlled manner and is answered by a ROUTE REPLY (RREP) packet from either the destination node or another node that knows a route to the destination. To reduce the cost of Route Discovery, each node maintains a cache of source routes it has learned or overheard.

Route Maintenance is the mechanism by which a packet's sender ***S*** detects if the network topology has changed. When Route Maintenance indicates a source route is broken, ***S*** is notified with a ROUTE ERROR (RERR) packet. The sender ***S*** can then attempt to use any other route to ***D*** already in its cache or can invoke Route Discovery again to find a new route.

III. MISBEHAVING NODES MODEL

Routing protocols provide two main functions: Routing function and data forwarding function. The former is concerned with routes discovery and routes maintenance. The latter is concerned with data packets relaying toward the destination through the established route. Both routing and data forwarding can be affected by misbehaving nodes presence; misbehaving nodes can lead the network into malfunction by not following routing and packets forwarding functions.

We consider two kinds of misbehaving nodes: selfish nodes and malicious nodes. We consider the following parameters that may govern the severity of an attack:

- *Time*: start and stop time,
- *Degree*: the probability (P) of misbehaviour,
- *Target*: victims' nodes (all nodes, a subset of nodes).

A. Selfish nodes

Selfish nodes try to save their own resources since resources are very constrained in wireless devices. So selfish nodes may decide to not consume their resource in forwarding data packets for other nodes: this can be achieved in two ways:

1) Selfish node type 1

Theses nodes participate correctly in routing function but not forward data packets it receive for other node; so data packets may be dropped instead of being forwarded to their destination.

2) Selfish node type 2:

Theses nodes do not participate correctly in routing function by not advertising available routes, for example: in DSR selfish node may drop all RREQ they received or not forward a RREP to some destination. Consequently, this selfish node will not participate in the requested routes.

B. Malicious nodes

Unlike, selfish nodes, malicious nodes don't preserve their resource and try to sabotage other nodes by trying to participate in all established routes. Consequently, the malicious nodes can force other nodes to use a "dangerous" route which is under their control. The manoeuvre that the malicious nodes may take is protocol-dependent. In the context of DSR routing protocol, a malicious node can claim to have a route to some destination and reply with false information to the received RREQ. After being selected in the requested route, it can cause DoS attack by dropping all the received packets, in Black Hole attack, or selectively dropping packets in Grey hole attack. Even more, malicious nodes can cause severe damage by collaborating in the attack, such as wormhole attack.

IV. SIMULATION

In order to measure the impact of selfish or malicious nodes on ad hoc network performances we modified the DSR implementation in (ns-2) [11] to simulate the different kinds of misbehaving nodes described in section III: selfish type1, selfish type 2 and malicious. First we present selfishness impact, then malicious node impact.

In our simulations, nodes move according to the random waypoint mobility model [2]. We use 30 or 60 mobile nodes that move in a rectangular surface of size 1000×1000 m² to increase the average number of hops per route, creating a more challenging environment for the routing protocol. The data communication pattern in our study uses 20 source-destination pairs, each sending a Constant Bit Rate (CBR) flow of 4 data packets per second. Each data packet is 512 bytes in size. All simulations were run on identical movement and communication scenarios. Simulations results have been plotted after taking an average of 10 simulations run. Table 1 resumes simulation parameters.

To measure the impact of misbehaving nodes we use two metrics:

- **Packet Delivery Fraction (PDF):** The fraction of the data packets generated by the CBR source that are delivered to destination.
- **Average End to End Delay (EED):** The average delay between the sending of data packet by the CBR source and its receipt by the corresponding receiver. This includes all delays caused during route acquisition and buffering at intermediate nodes

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Routing Protocol	DSR
Simulation time	500 seconds
Number of mobile nodes	30 nodes/ 60 nodes
Transmission Range	250 m
Movement Model	Random Waypoint
Pause time	10 seconds
Max speed	5 m/s
Traffic type	CBR
Data payload	512 bytes
Rate	2 packets/seconds
Target of attacks	All nodes
Time of attacks	500 seconds

A. *Simulation result of selfish behaviour*

Multiple selfish nodes may exist and operate independently in the network. We have developed a script that selects **m** nodes to be configured with the adequate selfishness type, time, degree and target.

The impact of the selfish behaviour is studied on two different scenarios: according to nodes density and probability of selfishness:

- In the first scenario we fix probability of selfishness to one (P = 1) and study the effect of selfish behaviour in High[1] and low[2] nodes density.
- In the second scenario we take a scene of 30 nodes (low density) and study the effect of selfish nodes in different probabilities (P) values.

Here we consider selfish nodes that behave according to selfish type 1 then selfish type 2 described in section III.A. Selfish nodes target all nodes during all simulation time. .

B. *Simulation results of selfish type 1*

As shown in figure 1, the percentage of selfish nodes has a significant effect on the fraction of packets that are successfully delivered in the network. The PDF decreases when the percentage of selfish nodes increases. We note that the selfish type 1 behaviour have the same effect on PDF in both low and high nodes density. However, as shown in figure 2, this effect decreases when the probability of selfishness type 1 decreases.

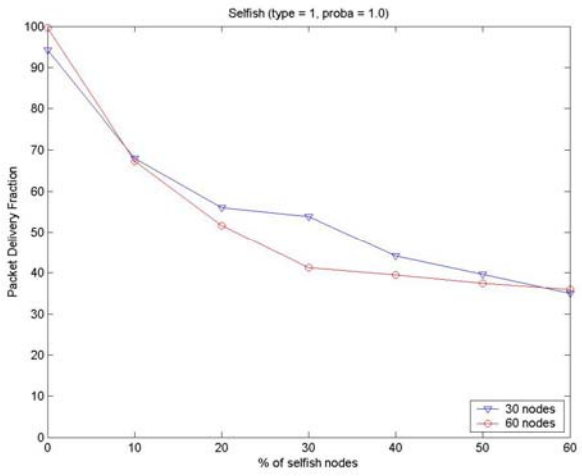

Figure 1. PDF vs % selfish nodes (type 1) in low and high nodes density

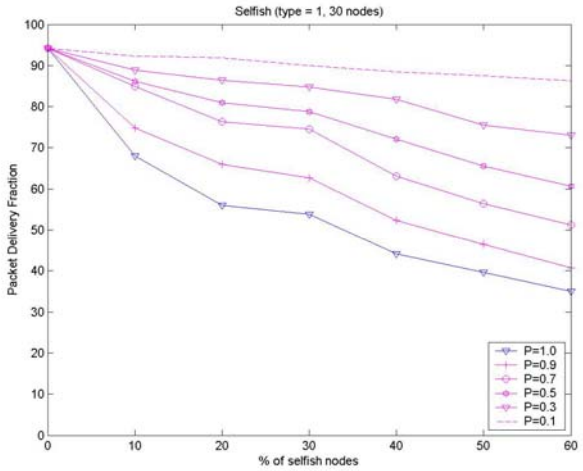

Figure 2. PDF vs % selfish nodes (type 1) of different P values

C. *Simulation results of selfish type 2*

Frome figure 3 and figure 4, we note that selfishness type 2 has not a big effect on PDF, especially in high nodes density. The reason is that selfish nodes that drop the received RREQ are avoided from participating in routes setup giving chance to other well behaving nodes to participate in the route construction. However, as shown in figure 4 and figure 5, selfishness behaviour type 2 can affect the average end to end delay by introducing long time buffering at intermediate nodes which cooperate in packet forwarding process. The average EED increases when the percentage of selfish nodes increases, especially in low node density.

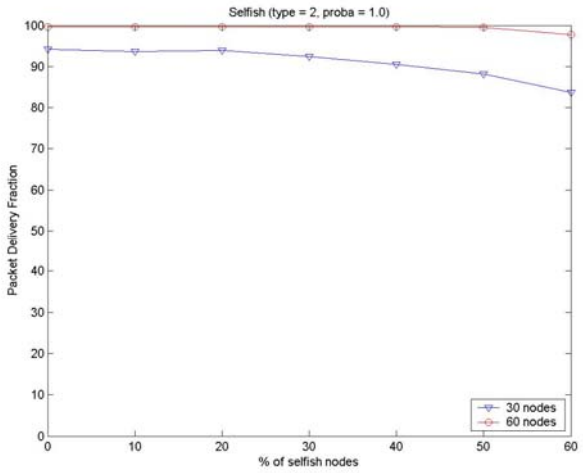

Figure 3. PDF vs % selfish nodes (type 2) in low and height nodes density.

[1] High nodes density means 60 nodes in a surface of 1000x1000 m
[2] Low nodes density means 30 nodes in a surface of 1000x1000 m

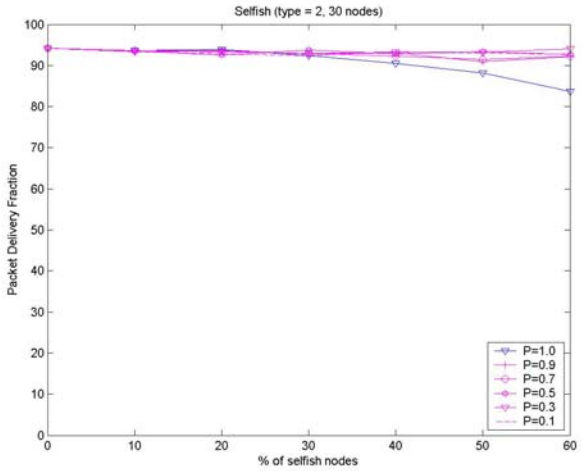

Figure 4. PDF vs % selfish nodes (type 2) of different P values.

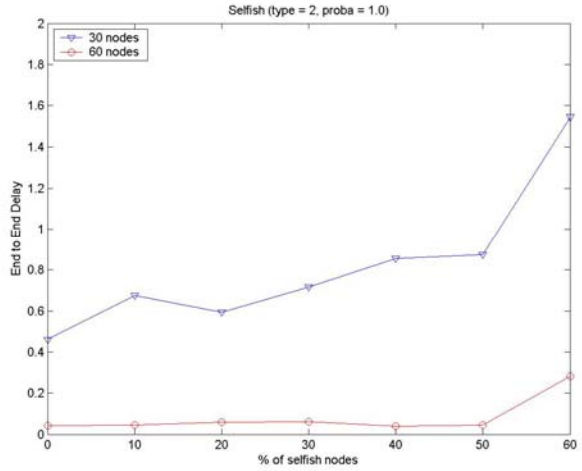

Figure 5. EED vs % selfish nodes (type 2) in low and height nodes density.

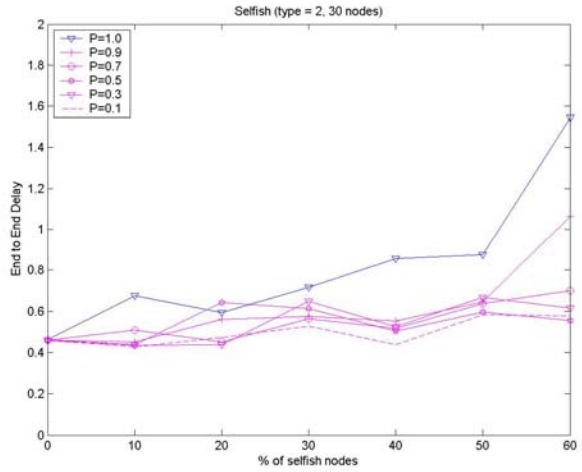

Figure 6. EED vs % selfish nodes (type 2) of different P values.

D. Simulation result of malicious behaviour

In this section we measure the impact of one malicious node performing black hole attack by varying nodes mobility and number of CBR connections. We consider one malicious node located in the center of the area of simulation that performs black hole attack to all nodes (degree =1.0) during all period of simulation.

One problem with route discovery process in DSR is that not only the destination node can send a route reply message (RREP); it is also possible that a node in the middle knows a valid route and can send an RREP message back to the sender. When a malicious node receives a route request message (RREQ), it sends a forged RREP packet back to the source node that initiates a route discovery, pretending that the destination node is only one or few hops away from it, and consequently drops all data traffic from the source node.

From figure 7 and 8, we can see that the PDF falls to 55% - 60% when only one malicious node performs the *black hole* attack. This result persists in different mobility and data traffic loads. The reason is that the malicious node position (in the centre) gives it more chance to participate in all routes by advertising forged RREP, and consequently preventing other nodes from discovering optimal routes. *Gray hole* attack which is a variant of black hole attack can have little impact on PDF by selectively dropping data traffic.

V. COUNTERMEASURES

Several works on securing ad hoc routing protocols have been proposed [12, 13, 14, 15]. A common approach towards secure ad hoc routing protocols is the use of cryptographic mechanisms to secure the ad hoc routing process. These approaches are built on different security assumptions, ranging from a single security association between the corresponding nodes to the assumption of an always available public key infrastructure to support cryptographic operations. Cryptographic approaches handle **active** attacks "*inject false routing information*" launched by malicious nodes on route discovery process. However, they do not address **passive** attacks "*silently drop packets*" from selfish nodes.

Other related works [16, 17] try to mitigate nodes misbehaviour using neighbours monitoring [18] to detect and isolate misbehaving nodes from a route. Nodes misbehaviour against which the proposals are targeted, have not yet been well described. Some works, such as Michiardi et al. [19] describe the influence of selfish nodes according to nodes energy. The underlying simulation approach, however, cannot be easily generalized. In our work we proposed a misbehaving node model including both selfish and malicious nodes enhanced with more action capabilities such as time of attack, target of the attack, degree (probability) of having a specific behavior. We evaluated the impact of this model on DSR performance trough different simulation scenarios.

We believe that a good countermeasure would be a combination of cryptographic and monitoring mechanisms in order to detect and isolate bisbehaving nodes.

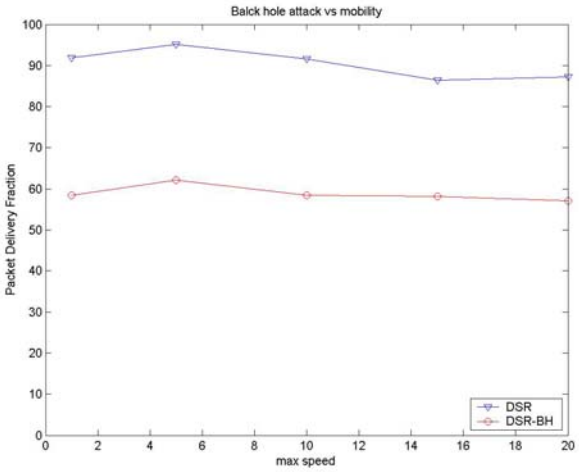

Figure 7. PDF vs max speed.

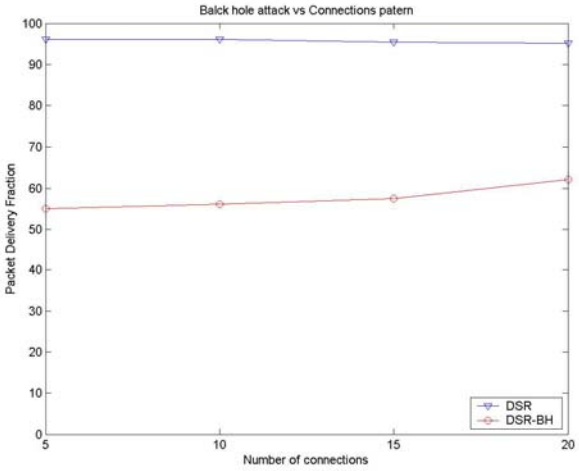

Figure 8. PDF vs number of CBR connections.

VI. CONCLUSION

Misbehaving nodes presence is one major security threat in MANETs that can affect the performance of the underplaying protocols. In this paper, we have studied the misbehaving nodes impact on MANET performance when DSR routing protocol is used. Similar results can be found when using AODV [20] routing protocol.

Through simulations, we have seen how much selfish and malicious nodes can affect network performance. Simulation results brought up two important conclusions:

- Selfish node type 2 (dropping RREQ) do not cause any damage in network with high nodes density. However, it can really affect the end to end delay and lead to congestion in a low density network.
- One malicious node carrying a balck hole attack can have the same effect as 20% to 30% of selfish nodes type 1 (Data dropping).

Therefore, both data and routing packets need to be secured from selfish and malicious nodes. We believe that a good solution would be a combination of cryptographic and monitoring mechanisms in order to detect and isolate misbehaving nodes.

REFERENCES

[1] S. Corson, J. Macker. "Mobile Ad hoc Networking (MANET) Routing Protocol Performance Issue and evaluation considerations". RFC 2501, January 1999.

[2] E.Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, Vol. 6, No. 2, pp.46-55. April 1999.

[3] J. Broch, D.A. Maltz, D.B. Johnson, Y. Hu, J. Jetcheva,"A performance comparison of multi-hop wireless ad hoc network routing protocols". In Proceedings of the Fourth Annual International Conference on Mobile Computing and Networking (MobiCom'98), ACM, Dallas, TX, October 1998

[4] D. Djenouri, A. Derhab, N. Badache."Ad Hoc Networks Routing Protocols and Mobility". Int. Arab J. Inf. Technol. (IAJIT) 3(2):126-133, 2006.

[5] D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007.

[6] The IETF Web site, http://www.ietf.org.

[7] F. Kargl, S. Schlott, A. Klenk, A. Geiss, M. Weber. “Securing Ad hoc Routing Protocols”. EUROMICRO 2004.

[8] A. Barbir, S. Murphy, Y. Yang, "Generic Threats to Routing Protocols". IETF RFC4593. Status Informational, October, 2006.

[9] Y. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy, pp. 28-39, 2004.

[10] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless/Mobile Network Security, Springer, 2008.

[11] NS2 network simulator. http://www.isi.edu/nsnam/ns.

[12] M. Zapata, "Secure Ad Hoc On-Demand Distance Vector (SAODV) ". Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.

[13] P. Papadimitratos, Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks", In Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January. 2002.

[14] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad hoc Networks", The 10th IEEE Intl. Conf. on Network Protocol (ICNP), Nov. 2002.

[15] Y. Hu, D. B. Johnson, A. Perrig, Ariadne, "A Secure On-Demand Routing Protocol for Ad Hoc Networks", Mobicom’02, 2002.

[16] S. Buchegger, J. Boudec, "Nodes Bearing Grudges: Towards Routing Security,Fairness, and Robustness in Mobile Ad Hoc Networks", In Proc. of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, January, 2002.

[17] P. Michiardi, R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks", IFIP-Communication and Multimedia Security Conference 2002.

[18] S. Marti, T. Giuli, K. Lai, M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", In Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MOBICOM), Boston, 2000.

[19] P. Michiardi, R. Molva. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks". European Wireless Conference, 2002.

[20] C. Perkins, E. Belding-Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing". RFC 3561, July, 2003.