A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack

Su Mon Bo, Hannan Xiao[1], Aderemi Adereti, James A. Malcolm and Bruce Christianson
School of Computer Science, University of Hertfordshire
College Lane, Hatfield, AL10 9AB, UK
Emails: h.xiao, j.a.malcolm, b.christianson@herts.ac.uk

Abstract

The unique characteristics of a mobile ad hoc network (MANET), such as dynamic topology, shared wireless medium and open peer-to-peer network architecture, pose various security challenges. This paper compares three routing protocols, DSDV, DSR, and AODV under security attack where two types of node misbehaviour have been investigated. Network performance is evaluated in terms of normalized throughput, routing overhead, normalized routing load, and average packet delay, when a percentage of nodes misbehave. Simulation results show that although the performance of all three routing protocols degrades, DSDV is the most robust routing protocol under security attacks. This reveals that a proactive routing protocol has the potential of excluding misbehaving nodes in advance and reducing the impact of security attack.

Keywords—wireless ad hoc networks, routing protocols, security attack

1 Introduction

A mobile ad hoc network (MANET) consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of any centralized administration or network infrastructure. The routing protocols in an ad hoc network should be able to cope well with dynamically changing topology, and nodes should exchange information on the topology of the network in order to establish routes. This brings about the issue of security in an ad hoc network. Using the wireless links in MANETs, any security gained because of the difficulty of tapping into a wired network is lost since the topology of MANETs is highly dynamic and traditional routing protocols can no longer be used. Due to the dynamic network topology, different packets exchanged between the same two nodes may go through different routes, among which there may be attackers lurking. It is also difficult to authenticate each node of a MANET unlike in a wired network, because of the absence of online servers [4]. Common security attacks include replay attack, denial of Service (DoS), modification, masquerading, routing table overflow, impersonation, energy consumption, and so on [2]. Some secure routing protocols have been proposed to protect routing messages and prevent attackers from either modifying these messages or injecting harmful routing messages into the network [4, 6, 7, 10].

A simulation-based analysis of security exposures in MANETs was carried out by Michiardi and Molva [5] where it is assumed that a node may misbehave under the above security attacks. Three types of routing misbehaviour have been classified and simulated within the dynamic routing protocol (DSR) [3]. Their simulation results showed that network operation and maintenance can be easily jeopardized and network performance severely affected. The objective of this paper is to extend this work to compare the performance under security attack of DSR with two other well-known ad hoc routing protocols: DSDV (Destination Sequenced Distance Vector) [8], and AODV (Ad hoc on Demand Distance Vector Routing) [9]. The performance of these routing protocols when security is not of concern has been extensively studied and compared previously [1]. It is interesting to see how robust each routing protocol's approach is against security attack.

In the rest of the paper, Section 2 briefly introduces the above three routing protocols and discusses the two types of routing misbehaviour. Section 3 describes the simulation environment and methodology in *ns2*. Section 4 presents the simulation results and discussion and finally, Section 5 concludes the paper.

2 Routing Protocols and Routing Behaviours

2.1 Routing Protocols

Routing protocols in MANETs are classified as table driven or on-demand. Table driven protocols are proactive, because they attempt to maintain consistent up-to-date information. On demand routing protocols are also known as reactive protocols which are source-initiated and create routes only when desired by a node. This paper compares

[1] Corresponding author

0-7695-2876-7/07 $25.00 © 2007 IEEE
DOI 10.1109/IAS.2007.35

one table driven routing protocol: DSDV and two prominent on-demand routing protocols: DSR and AODV.

DSDV: This routing protocol is a table-driven algorithm based on the Bellman-Ford routing mechanism. To avoid routing loops, every mobile node in the network maintains a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded. Entries are marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops.

DSR: This is a simple and efficient routing protocol composed of two mechanisms, route discovery and route maintenance, which work together to allow nodes discover and maintain source routes to arbitrary destinations in the ad hoc network. The source node uses Route Discovery to find a route when a request arrives and inserts the discovered routes in the packet header. Intermediate nodes do not need to maintain up-to-date routing information apart from participation in the route discovery and maintenance.

AODV: The AODV routing protocol is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node.

2.2 Routing Misbehaviours

Misbehaviour of nodes has been used to distinguish networks that are under security attack. Previous work has pointed out two types of misbehaviour: a selfish behaviour and a malicious behaviour [5]. Selfish nodes use the network but do not cooperate, saving battery life for their own communications: they do not intend to directly damage other nodes. Malicious nodes aim at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority. This paper focuses on the misbehaviour model for selfish nodes and based on [5] defines two different type models for them. Node selfishness is of great interest because nodes of MANETs are often battery-powered, thus energy is a precious resource that they may not want to waste for the benefit of other nodes. All together we define three routing behaviours of nodes.

1) Type 0 well-behaved node: Nodes behave nicely according to a routing protocol including route discovery, maintenance, packet forwarding and receiving.

2) Type 1 selfish node: In this model, a selfish node does not perform packet forwarding, so every packet sent to this node is dropped by it. Thus, it disables the packet forwarding function for all packets that have a source address or a destination address different from the current selfish node address. This actually helps the selfish node in terms of consumed energy to save a significant portion of its battery life by neglecting large data packets, while still contributing to the network maintenance.

3) Type 2 selfish node: In this model, the node does nothing with the packet sent to it, thereby no execution function is performed. The selfish node can be considered as a rest node inside the network, since it stops contributing to the network maintenance, routing discovery, nor packet forwarding and receiving.

We believe that these selfishness models are simple, but realistic. Our following simulation study evaluates the performance of DSDV, DSR and AODV when a certain percentage of nodes behave following the Type 1 and Type 2 selfishness models above, while the remaining nodes are assumed to be well-behaved.

3 Simulation Environment and Methodology

ns2 provides a good platform for MANET simulation. It contains models and modules at physical and data link layers, medium access control protocols, and the ad hoc routing protocols we want to compare (DSDV, DSR and AODV). The node movement scenario allows a node to choose its destination and moves towards it at a uniform speed. This is called the random *waypoint* model. When a node reaches its destination it waits for a pause time before choosing a random destination and repeating the process. Communications among randomly selected nodes are established using constant bit rate (CBR) traffic. The above node misbehaviours have been added as separate node definition types in the *ns2* node model, which allows selection of selfishness model between two possible choices. Using the *ns2* environment, some common parameters are listed in Table 1.

Parameters	Values
Area	1000m x 1000m
Radio range	250 m
Link capacity	2 Mbps
Pause time	5 seconds
Simulation time	200 seconds
Buffer size	50 packets
Application	Constant bit rate (CBR) traffic
Packet size	512 bytes

Table 1. Fixed parameters in simulation

Apart from the above fixed parameters, we design the simulations by changing certain aspects of MANETs in order to evaluate the network performance of routing protocols under security attack. As summarised in Table 2, the aspects are as follows:

Network Density: This aspect is represented by the num-

Parameters	Values
Network density	high (60 nodes) / low (20 nodes)
Network mobility	high (15 m/s) / low (2m/s)
Routing protocols	DSDV / DSR / AODV
Types of selfish node	Type 1 / Type 2
Percentage of SNs	0-50%

Table 2. Variable parameters in simulation

ber of nodes in a fixed area where an MANET is run. Two kinds of densities are considered: high density refers to the usage of 60 nodes in an area of 1000m x 1000m, and low density 20 nodes in the same area. The denseness of a node in a MANET would influence the performance of the routing protocols used in the network. Thus, it should be expected that an increased density of nodes in the network would decrease the routing protocols performance as a direct effect of less bandwidth and higher congestion but might also reduce the deleterious effect of selfish nodes.

Network Mobility: Two types of network mobility scenarios are simulated. Within a high mobility network, all nodes move with a maximum speed of 15 m/s while within a low mobility network, all nodes move with a maximum speed of 2 m/s. The performance of routing protocols will be worse under high network mobility.

Routing protocols: Three types of ad hoc routing protocols are used: DSDV, DSR and AODV.

Types of selfish nodes: As described in the last Section, two types of selfish nodes are simulated: Type 1 and Type 2. It is expected that Type 1 selfish node may degrade the network more than Type 2 as it participates in routing discovery and maintenance but refuses to forward packet when it is included in a route.

Percentage of selfish nodes: The network will suffer more when more well-behaved nodes are compromised to selfish nodes. The number of selfish nodes is presented by percentage, from 0% to 50%. The remaining nodes are assumed to be well-behaved.

3.1 Performance metrics

In comparing the protocols, network performance is evaluated according to the following metrics:

Normalized throughput: Also called packet delivery ratio in [1] and throughput in [5], this is the ratio of the number of packets received by the CBR sink to the number of packets sent by the CBR source, both at the application layer. Packets that are sent but not received are lost in the network due to malicious drops, route failures, congestion, and wireless channel losses.

Average delay: This is the average delay of all the packets that are correctly received. Lost packets are obviously not included in this measurement since their packet delay is infinity.

Routing overhead: The total number of routing packets transmitted during the simulation at the network layer. Packets that are routed over multiple hops are counted multiple times – each hop is counted as one transmission.

Normalized routing load: The ratio of the total number of routing packets transmitted or forwarded at the network layer to the total number of CBR packets received at the destination at the application layer.

These metrics together give a thorough evaluation of a routing protocol. Normalized throughput represents both the completeness and correctness of the routing protocol; average packet delay tells efficiency of the protocol to correctly deliver packets and the degree of network congestion; routing overhead measures the scalability of the routing protocol and its power consumption efficiency; and normalized routing load demonstrates to some extend the average number of hops the protocol routes a packet from sender to receiver, as well as the efficiency of the protocol.

4 Simulation Results and Analysis

In this paper, only simulation results of network with low node density are presented and discussed. Figures 1, 2, 3, and 4 demonstrate the results of normalized throughput, average delay, routing overhead and normalized overhead of networks with low node density, low / high node mobility, and Type 1 / Type 2 selfish nodes. Overall, DSR and AODV suffer a lot from the two types of selfish nodes, while DSDV shows constant performance under security attack although its performance also degrades. We do not compare the performance between Type 1 and Type 2 selfish nodes since our interest is in comparing the routing protocols.

4.1 Normalized Throughput

Fig. 1 presents the normalized throughput of DSDV, DSR and AODV, with low node density, low / high node mobility, and increasing percentage of selfish nodes of Type 1 and Type 2. In a low mobility network, when there is no selfish nodes in the network, DSR and AODV achieve higher throughput (i.e., deliver around 80% of the offered load) than DSDV (which delivers just about 60% of the offered load) (see Figs. 1a and 1b). The throughput of all the three protocols declines when the percentage of selfish nodes increases. In a high mobility network, the impact of selfish nodes in DSDV throughput is not very strong with a quite constant value between 10% to 30% normalized throughput (see Figs. 1c and 1d). On the other hand, the normalized throughput of AODV and DSR drops quickly: for AODV from about 70% to about 10%, and for DSR from about 60% to about 10%.

This is because the selfish nodes in the network do not cooperate well in the protocols as well-behaved nodes: Type 1 nodes do not forward packets for other nodes while Type 2 nodes do not participate in any routing activity. As a result, the network malfunctions, with decreasing efficiency of packet delivery.

4.2 Average Packet Delay

Fig. 2 shows the average packet delay of DSDV, DSR and AODV with low node density, low / high node mobility, and increasing percentage of selfish nodes of Type 1 and Type 2. The impacts of selfish nodes on delay for the protocols are not very obvious, apart from an increase trend for DSR under low mobility with Type 2 selfish node (see Fig. 2b), and for AODV under high mobility with Type 2 selfish node (see Fig. 2d).

What is observed instead is that DSR always has a higher average packet delay among the three protocols and DSDV the lowest with or without selfish nodes. This is because DSR needs time to find a route on demand of the source, or when the link breakage happens; while DSDV is a proactive routing protocol and finds route periodically, thereby a route is ready when a packet is required to be sent, reducing the packet delay. As a combination of DSR and DSDV, AODV results in a modest packet delay in the middle, as shown in Figs. 2a, 2b, 2c, and 2d.

4.3 Routing Overhead

Fig. 3 shows the routing overhead of DSDV, DSR and AODV with low node density, low / high node mobility, and increasing percentage of selfish nodes of Type 1 and Type 2.

In the low mobility case, the routing overhead of AODV decreases quickly from about 45000 packets when there is no selfish nodes to about 15000 packets when there is 10% of selfish nodes (see Figs 3a and 3b), and then drops less severely when the percentage of selfish nodes increases. A similar trend is observed for DSR. This is because as the normalized throughput of DSR and AODV suffers from the selfish nodes (see Fig. 1), more packets are dropped in the network thus requiring less routing overhead. In contrast, DSDV keeps a approximately constant overhead regardless the existence of selfish nodes and how many of them. This is because DSDV is table-driven with relatively stable routing control overhead, as also observed in Fig. 1 that the normalized throughput of DSDV changes less than those of DSR and AODV.

In the high mobility case, again the overhead of DSR and AODV decreases with the increase of selfish nodes but that of DSDV is approximately constant (see Fig. 3c and 3d).

4.4 Normalized Routing Load

Fig. 4 shows the normalized routing load of DSDV, DSR and AODV with low node density, low / high node mobility, and increasing percentage of selfish nodes of Type 1 and Type 2. No constant trend is observed for AODV. For example, with low mobility, apart from when there is no selfish node, the normalized routing load of AODV shows an increase trend with the increase of Type 1 selfish nodes (see Fig. 4a), but this trend does not hold with the increase of Type 2 selfish nodes (see Fig. 4b), nor with the high mobility case (see Figs. 4c and 4d). No obvious trend is observed for DSR either. For DSDV, there is a slightly increase trend of normalized routing load with the increase of selfish nodes (Figs. 4a, 4b, 4c, and 4d). This means that packets travel through more hops to reach destinations when more nodes are compromised.

Another observation is that AODV normally has the highest normalized routing load among the three protocols and DSDV the least with or without selfish nodes. This shows that DSDV is the best in finding routes optimal to the shortest paths.

5 Conclusion and Future Work

This paper compares three routing protocols, DSDV, DSR, and AODV under security attack. Network performance is evaluated in terms of normalized throughput, average packet delay, routing overhead and normalized routing load, when a percentage of nodes behave selfishly. Simulation results show that although the performance of all three routing protocols degrades, DSDV is the most robust routing protocol under security attack. This reveals that a proactive routing protocol has the potential of excluding misbehaving nodes in advance and reducing the impact of security attacks. In the future, we will compare the performance of routing protocols with different types of selfish nodes in a bigger area with longer simulation time with different node pause time. We will also study the robustness of DSDV and find a way of detecting misbehaving nodes in MANETs.

References

[1] J. Broch, D. A. Maltz, D. B. Johnson, Y. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *MobiCom '98: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pages 85–97, New York, NY, USA, 1998. ACM Press.

[2] H. Deng, W. Li, and D. P. Agrawal. Routing security wireless ad hoc networks. *IEEE Communications Magazine*, 2(1), 2002.

[3] D. B. Johnson. Routing in ad hoc networks of mobile hosts. In *IEEE Workshop on Mobile Computing Systems and Applications*, pages 158 –163, December 1994.

[4] H. Li and M. Singhal. A secure routing protocol for wireless ad hoc networks. In *HICSS'06: Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, page 225.1, Washington, DC, USA, 2006. IEEE Computer Society.

[5] P. Michiardi and R. Molva. Simulation-based analysis of security exposures in mobile ad hoc networks. In *Proceedings of European Wireless Conference*, 2002.

[6] P. Papadimitratos and Z. J. Haas. Securing routing for mobile ad hoc networks. In *Proceedings SCS (CNDS2002)*, 2002.

[7] K. Paul and D. Westhoff. Context aware detection of selfish nodes in DSR based ad-hoc networks. In *IEEE GLOBECOM 2002, Taipei, Taiwan*, November 2002.

[8] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM '94*, pages 234–244, London, England, August 1994.

[9] C. E. Perkins and E. M. Royer. Ad hoc on-demand distance vector routing. In *IEEE WMCSA'99*, pages 90–100, New Orleans, 1999.

[10] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based intrusion detection system for AODV. In *SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 125–134, New York, NY, USA, 2003. ACM Press.

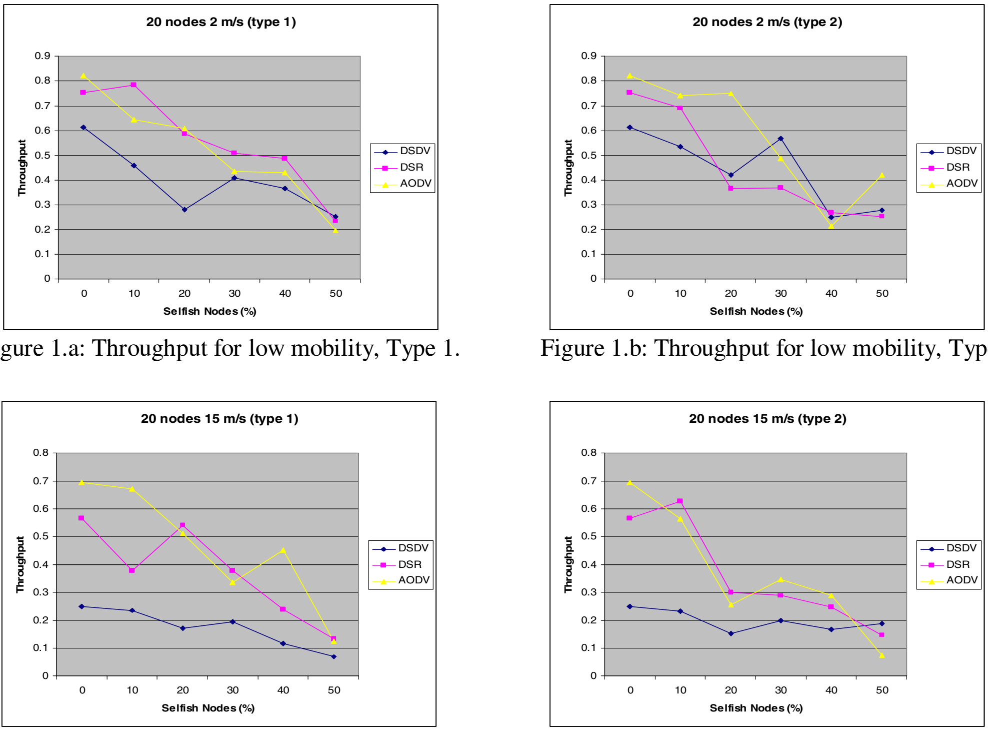

Figure 1.a: Throughput for low mobility, Type 1.

Figure 1.b: Throughput for low mobility, Type 2.

Figure 1.c: Throughput for high mobility, Type 1.

Figure 1.d: Throughput for high mobility, Type 2.

Figure 1: Normalized throughput under the low density, low mobility case, and the low density, high mobility case, with increasing percentage of selfish nodes of Type 1 and Type 2.

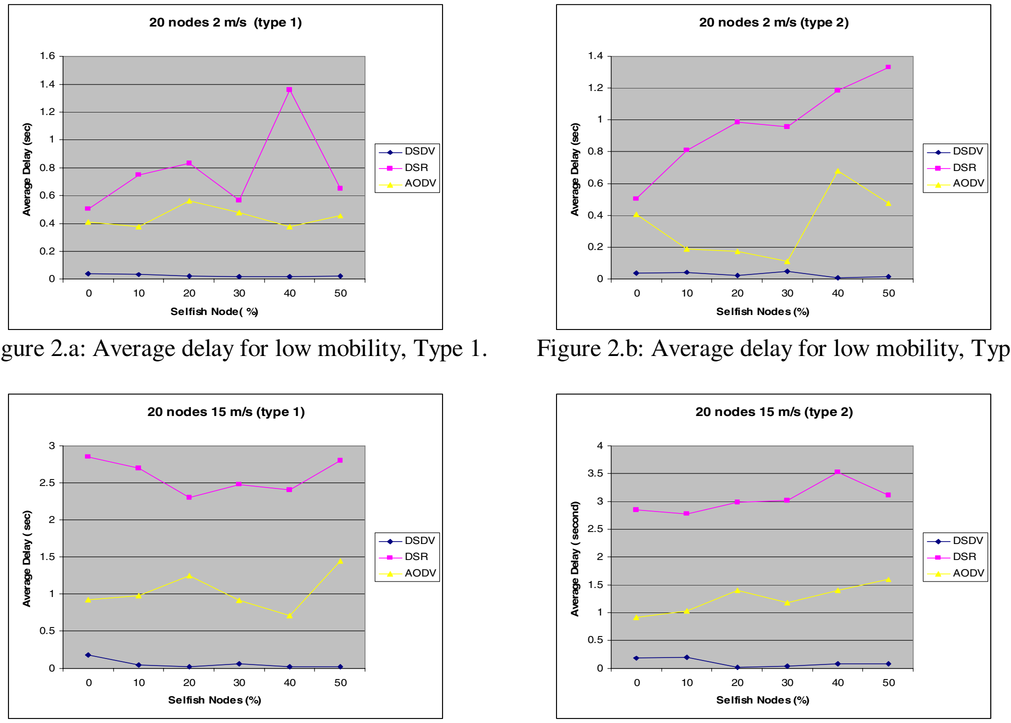

Figure 2.a: Average delay for low mobility, Type 1.

Figure 2.b: Average delay for low mobility, Type 2.

Figure 2.c: Average delay for high mobility, Type 1.

Figure 2.d: Average delay for high mobility, Type 2.

Figure 2: Average packet delay under the low density, low mobility case, and the low density, high mobility case, with increasing percentage of selfish nodes of Type 1 and Type 2.

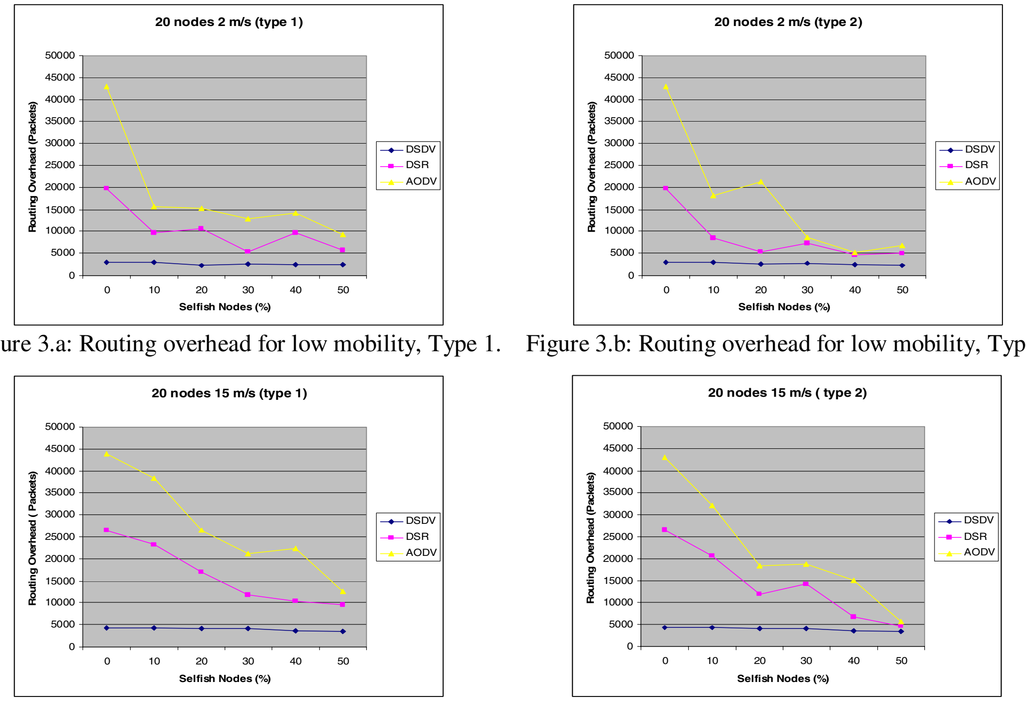

Figure 3.a: Routing overhead for low mobility, Type 1.

Figure 3.b: Routing overhead for low mobility, Type 2.

Figure 3.c: Routing overhead for high mobility, Type 1.

Figure 3.d: Routing overhead for high mobility, Type 2.

Figure 3: Routing overhead under the low density, low mobility case, and the low density, high mobility case, with increasing percentage of selfish nodes of Type 1 and Type 2.

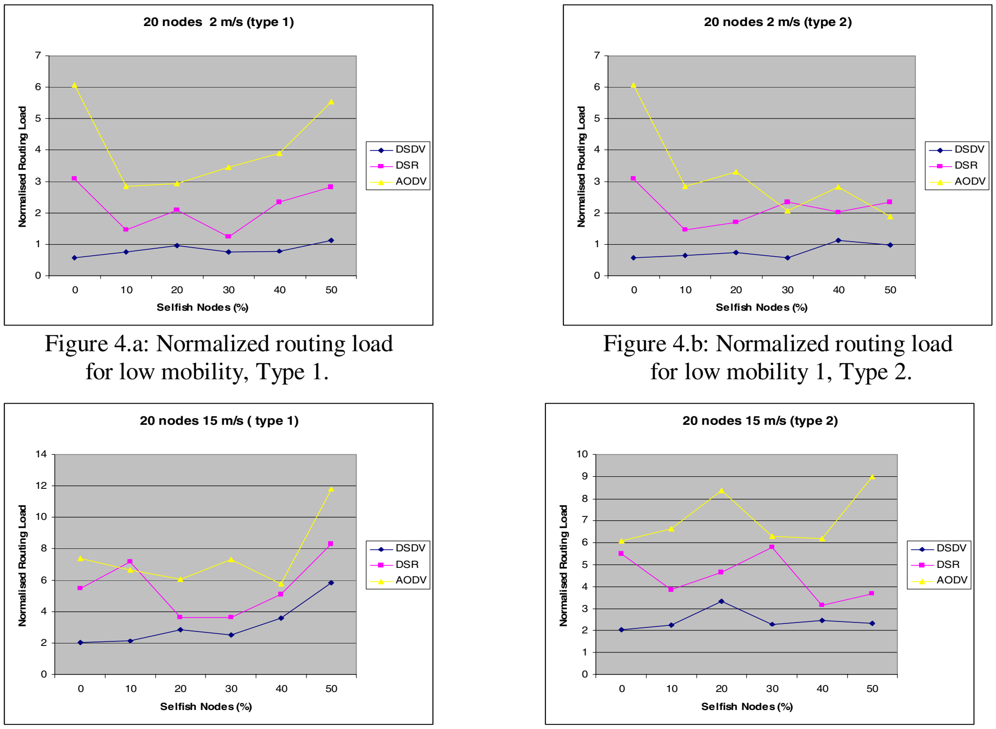

Figure 4.a: Normalized routing load for low mobility, Type 1.

Figure 4.b: Normalized routing load for low mobility 1, Type 2.

Figure 4.c: Normalized routing load for high mobility, Type 1.

Figure 4.d: Normalized routing load for high mobility, Type 2.

Figure 4: Normalized routing load under the low density, low mobility case, and the low density, high mobility case, with increasing percentage of selfish nodes of Type 1 and Type 2.