Reliability & Performance Limitations of AODV Ad-Hoc Networks

1.Introduction

Introduction

This research project was carried out as part of the University Research Scholarship Scheme with the aim of identifying the limitations of Ad-hoc Networking Protocols used in wireless networking, specifically looking at the issues related with the Adaptive On-Demand Distance Vector (AODV) protocol.

What is an Ad-hoc Network?

An Ad-hoc network is a dynamic network primarily composed of mobile computers. They provide flexible networks where conditions do not necessarily warrant or support a wired communication infrastructure. The uptake of such networks has accelerated recently due to the decreasing costs for the technology.

What is AODV?

AODV is designed to allow many low power, limited memory mobile devices to create adaptive networks without utilising excessive network bandwidth in order for the devices to share electronic resources.

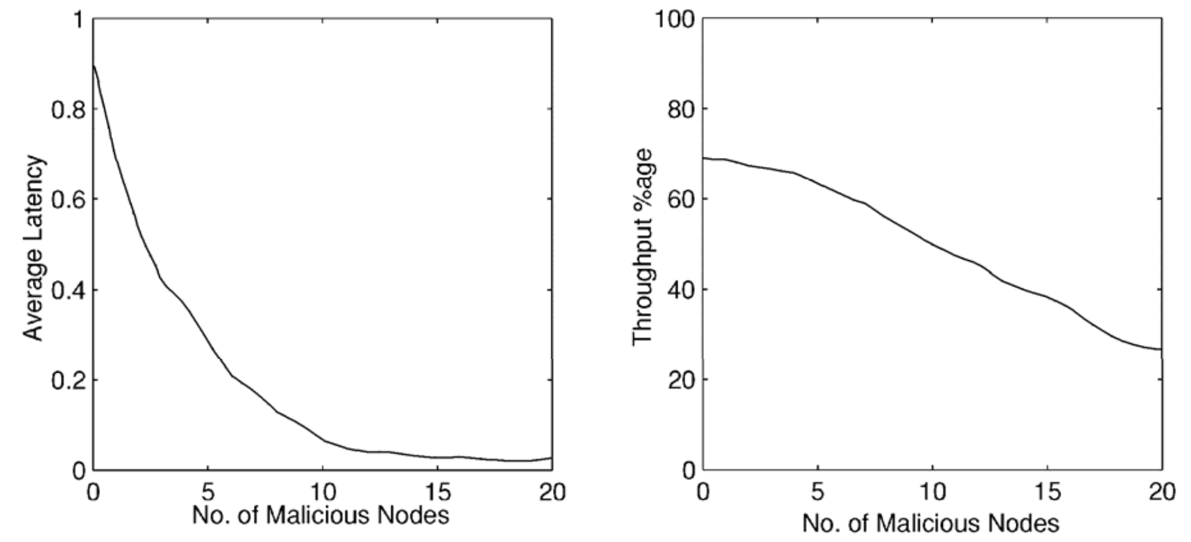
2.Previous Research

About Previous Research

There has been very little research carried out into Ad-Hoc networking protocols, however A.A.Pirzada has carried out some research in this area focusing on AODV and DSR.

Findings

Some of the findings shown within the papers by A.A.Pirzada indicated some unusual behaviour for which no reasons were given. Some of these graphs are shown below and highlighted in the following section.



Unexpected Results

The main issue with the results was that the data showed the average latency of the network to decrease with more malicious nodes. This is deemed a good response but comes unexpectedly and it was later found that this gain came at a cost. The reasons for these results were discovered as a part of this research.

Acknowledgments

I would like to acknowledge the work of Anthony Dawson, my research partner during this project for all of his help in researching AODV and analysis of the results collected. In addition I would also like to acknowledge Arshad Jhumka and Nathan Griffiths for giving me the opportunity to take part in this research and for their help and advice throughout.
For more information on this project, NS2, AODV and contact details for Anthony and myself visit the following website http://www.dcs.warwick.ac.uk/~adhoc1/

Poster Created by Richard Myers for URSS 2007

3.The Testing

Types of Attacks

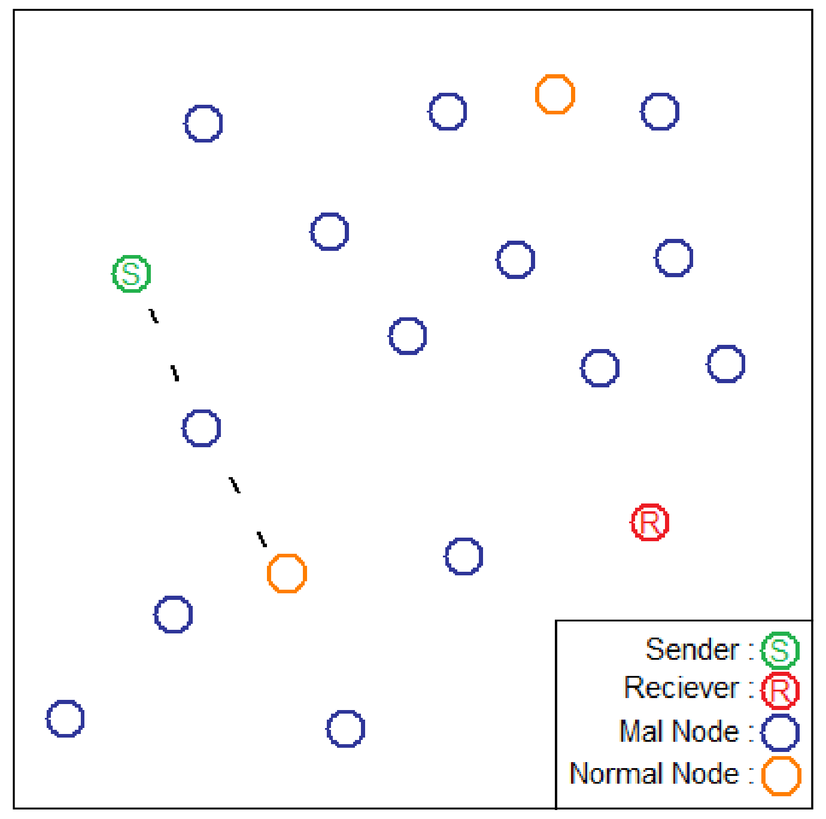
Having reviewed the research carried out previously four possible attacks/faults were decided upon. In the end the first three listed below were analysed while the fourth remains to be tested. The attack types selected were:

- **BlackOnRoute** - This attack sends fake messages that the node is on a route to the destination and then if data passes over them they simply drop these data packets preventing the receiver receiving them.
- **BlackFakeDst** - This acts very much like the BlackOnRoute above but this time rather than replying that it's got a route it replies with a message indicating it has the best route to the receiver
- **Greyhole** - This type of node is a faulty node which can intermittently stop relaying any types of messages for a random period of time. This is essentially a device with a faulty antenna.
- **Modification** - A modification device would modify some part of the data it is to forward. This could be caused maliciously or by a faulty device.

Test Types

Testing was carried out using two different environments. These were fully random environments in which all nodes within the network moved around using pseudo random movements with a varying speed and direction. Also tested was a static environment in which all the nodes moved as in the random environment except for the sender and receiver nodes which were placed on the edges of the environment and could not move.

The image to the *right* shows a specific moment in time during a small network simulation. You can see that the black dashes (data) make it to the orange malicious device and stop. They do not make it to the destination (red) as the malicious node is dropping these data packets.



Testing Strategy

The testing made use of a number of different technologies in order to produce reliable results. Therefore the following were used in testing:

- Network Simulator 2 (NS2) - An open source network simulation tool which could be extended for our purposes
- Condor - A grid computing environment of 100+ machines to allow for large numbers of simulations to be run simultaneously
- Custom Java Applications - Coded for use specifically for the project , including test creation and data analysis systems.

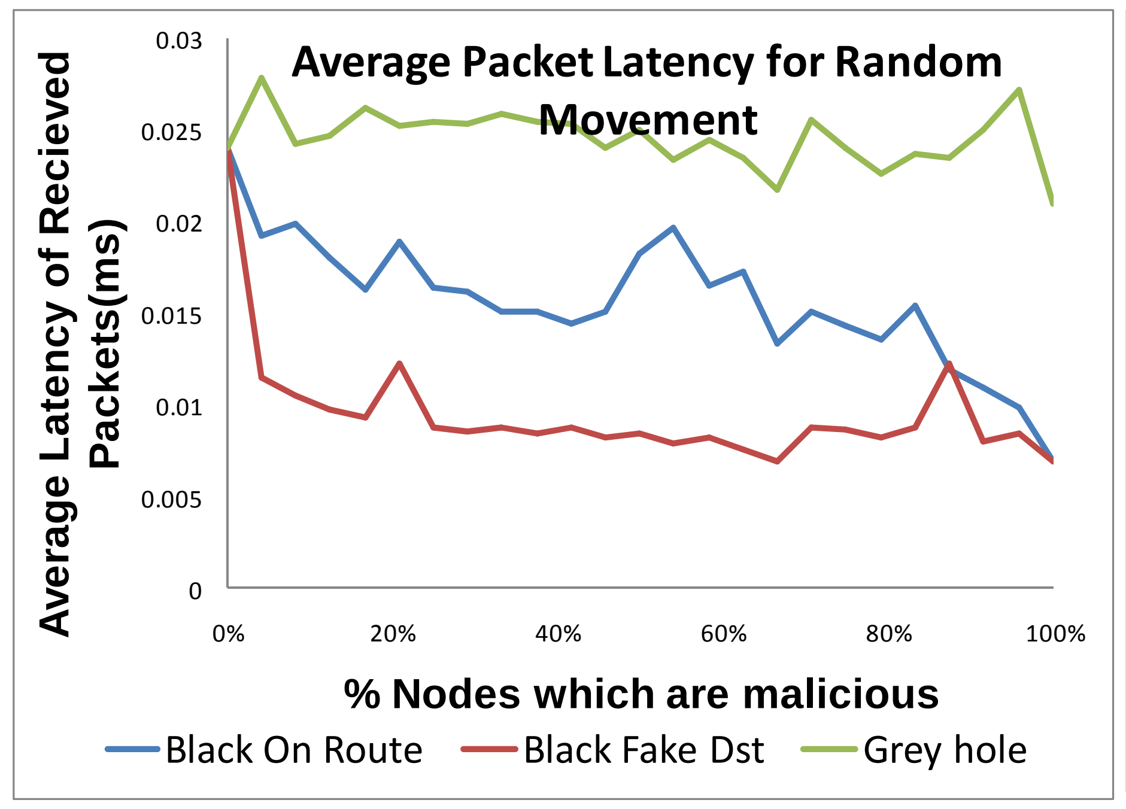
Each of the tests were configured and run using the same key setup :

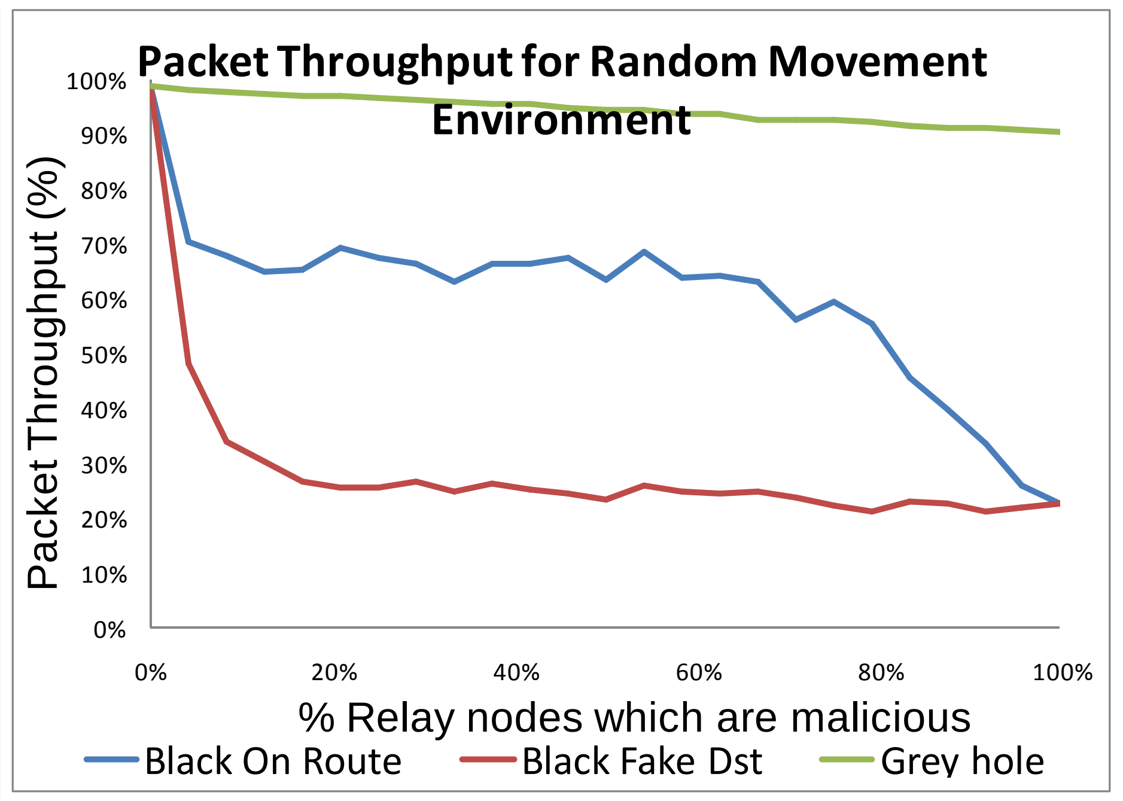
- Each test contained 50 nodes in total with normal nodes being replaced by malicious nodes after each major test
- Each major test consisted of 75 minor tests
- Each minor test lasted 15 minutes
- The nodes could move within a 1000x1000 metre environment with each node taking a pseudo random movement which was different for each minor test and then repeated again in each major test.

4.The Results

The Results

The results of the simulations generally agreed with those previously collected but also gave more detailed information having been carried out with smaller steps of precision and including the whole spectrum from no malicious nodes to the network being totally filled with malicious nodes. Also with the aid of the visual network replays it became possible to study what was actually going on in the network and this helped to explain the unexpected results. The following results show data collected from the random movement environment tests.





About the Results

The above two graphs highlight the key findings of this research. They confirm that average latency does decrease with more malicious nodes, although by looking at the packet throughput we can see that this occurs because so many packets get dropped by malicious nodes. Therefore the only time messages get sent successfully is when the sender and receiver are in direct communication and hence have the lowest latency. The results also suggest that with very few extremely malicious nodes the performance of the ad-hoc network can be greatly reduced. Also with these nodes being capable of receiving these messages it also opens up a number of security issues as this data could also be read by a malicious user who may retrieve usernames and passwords or other private data.

5.Conclusion

Research Conclusion

The results of the research can clearly show that the introduction of a number of highly malicious devices (ie. Those using the Fake Destination attack) could lead to the performance and reliability of an Ad-Hoc networking using AODV (and likely other Ad-hoc protocols) greatly decreasing. Therefore with more and more users relying on wireless networking it will be important to look for ways to detect these malicious devices

Further Areas of Research

Having completed this research there is more research which could continue on from this work and make use of the tools which have been put in place including :

- Analysis of the affects of Modification Attacks to network performance
- Building trust into AODV in order to detect and bypass malicious nodes. See second poster for more about this.

My Experience with URSS

Having taken part in URSS I have been able to gain a greater understanding of the activities involved in research-led work. It has also allowed me to learn new skills and improve many others. In addition I feel that we have been able to put in place a good grounding for future research into ad-hoc networking here at Warwick University.