Trusted AODV

Introduction

Wireless communications have become more prominent in recent years with the increased performance and affordability of wireless devices. This has led to the development of ad hoc networking protocols, such as AODV, which take full advantage of the mobility of wireless devices. These protocols work by allowing individual devices to be independent and interconnect in an ad hoc fashion. This has the advantage of high dynamicity, but before such protocols can be used commercially the security of such networks needs to be evaluated.

This project is the starting block for such research within The University of Warwick Computer Science department. With a long term aim, to participate in the research of trusted ad hoc networking protocols for commercial purposes.

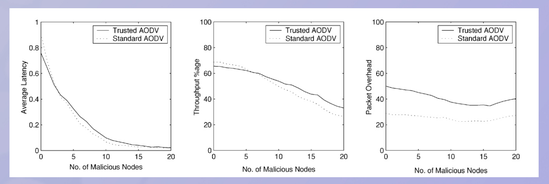
This project has been split into two composite parts of which this is the latter and consequently further background to ad hoc networking and the start of this project is detailed in the poster entitled “Reliability & Performance Limitations of AODV Ad-Hoc Networks”.

Aim

The aim of this project was to investigate and further the results produced in papers by A. A. Pirzada (A founding researcher within the area of trusted ad hoc networking). The reason for this was because the results described within his papers “Incorporating trust and reputation in the DSR protocol for dependable routing” [2] and “Trust Establishment In Pure Ad-hoc Networks” [3] appear unintuitive. To achieve this, trusted versions of both DSR and AODV (two substantially different ad hoc networking protocols) would have to be implemented. This cleanly split the overall project into two individual projects, one for each protocol. The two projects soon merged into one project focusing on the AODV protocol due to time constraints and difficulties with the DSR protocol.

Research within the area

The area of trusted ad hoc networking is a fairly new area of research and subsequently there are limited experimental results within this area. The majority of experimental results that do exist have been produced by A. A. Pirzada. The results in the following graphs are those that were of most interest to the project.



These results were taken from [3] and show how Trusted AODV performs in comparison to Standard AODV, for a random movement test. During a random movement test all the nodes within the network move randomly during the test, as to simulate the movement of node in a physical ad hoc network. All of the graphs are plotted against increasing numbers of malicious nodes.

These graphs show some unexpected trends; primarily it would not be expected for the Trusted AODV and Standard AODV to follow similar trends should the trust model be function correctly. With Trusted AODV showing a negligible performance benefit for the two most important network statistics throughput and average latency.

Throughput: is the percentage of data packets that successful made it from source to destination during the test.

Average Latency: is the average time it takes a packet to travel from source to destination.

Another unusual trend is apparent in the average latency graph, why does the average latency of the network decrease as a larger proportion of the network is malicious? This is not expected as lower latency is beneficial and this is not logical to expect with a higher number of malicious nodes. The reason for this did become apparent during the research.

Developing Trusted AODV

To be able to understand the results presented by A. A. Pirzada and research further into trusted ad hoc networks, it was necessary to develop a version of Trusted AODV. This was created using the NS-2 network simulator as used by Pirzada, to allow us to attempt to replicate his results.

What is Trust?

The concept of trust is the same as within real life, where you trust people that have been helpful and acted trustworthily towards you in the past. In the case of ad hoc networking, nodes that operate the protocols correctly are trusted. The purpose of developing a notion of trust within an ad hoc network is to provide a heuristic for security. Allowing faulty or malicious nodes to be detected and removed from the network, with minimal overhead and restriction to the network.

How can ad hoc trust be evaluated?

Trust in real life is evaluated on past experience of the person and your general feeling about them. Within an ad hoc network a nodes trust can be evaluated from a number of means.

Acknowledgement: This is where the node being trusted to perform a task is monitored to ensure it does. When a node has shown benevolent actions, trust in that node is increased.

Packet Precision: This is where a node entrusted to forward a packet is monitored for its accuracy. This ensures the packets are forwarded correctly.

Blacklists: Ad hoc protocols maintain a list of nodes that are blacklisted due to poor connectivity and are inherently less trusted.

Hello Packets: Hello messages are simply a periodic message broadcast by a node. With the purpose of indicating to neighbouring nodes its availability. This allows the most recently seen nodes to be more trusted.

These means can then be weighted and combined to create an overall trust level for a node.

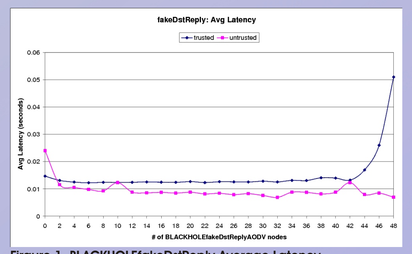
Trust in Trusted AODV

For the initial implementation of trusted AODV a basic trust model was implemented using purely acknowledgement as a means of evaluating trust. To achieve this a buffer of packets recently sent for forwarding was stored. This buffer could then be compared against the packets received from promiscuous mode, which is a means by which a wireless device can intercept any packet in range irrelevant of its source or destination. This allows Trusted AODV to check that the packets it entrusted to another node to forward were forwarded by that node.

The trust level was maintained using a simple counter, which was initialised to zero. The counter was incremented when a forward was acknowledged and decremented on failure. The counter was set to have a cut off -10, and nodes which reached this value were permanently banned from the network. This trust model although very simple provides a good starting point and proof of concept.

Results

These results compare the standard implementation of AODV within NS-2 to the performance of Trusted AODV using the very basic trust model. These results are for a random movement test against increasing numbers of malicious BLACKHOLEfakeDstReply nodes. These are the most malicious nodes that were created during the project for testing purposes and clearly highlight the importance of incorporating trust into ad hoc networks, as even a very basic model can have substantial results. This test was designed to generate results similar to the results produce by Pirzada, although it is not possible to determine the exact setup used from Pirzada's work.



Firgure 1, BLACKHOLEfakeDstReply Average Latency

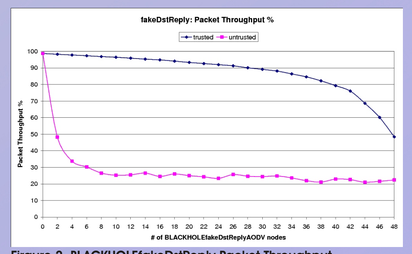
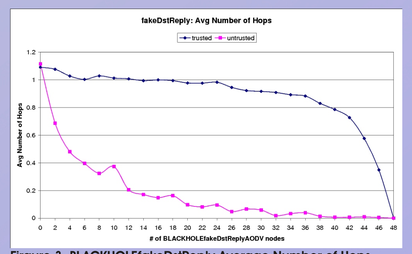


Figure 2, BLACKHOLEfakeDstReply Packet Throughput



Firgure 3, BLACKHOLEfakeDstReply Average Number of Hops

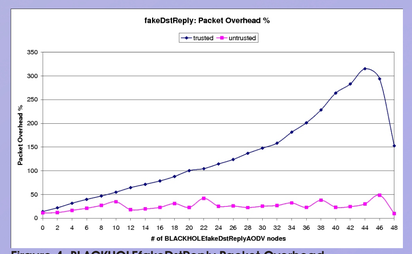


Figure 4, BLACKHOLEfakeDstReply Packet Overhead

Average Latency Results: Figure 1

The average latency between sender and receiver is the average time it takes for a message to be sent from sender to receiver, and is important to note that this does not include packets that have been lost, in this case most likely due to malicious nodes. This is the reason why latency appears to improve with increasing numbers of malicious nodes, because packets on longer routes have a higher probability of being dropped by a malicious node, biasing the average.

It can be seen that our implementation of Trusted AODV does not follow the same trend as AODV, remaining consistent until the network becomes saturated with malicious nodes. This causes packets to take consistently longer paths, as well as being buffered longer waiting for a suitable route in order to avoid malicious nodes. This can be seen within the average number of hops, with messages sent by trusted nodes clearly taking consistently longer routes, and is the result we expected. This is contrary to the results by Pirzada, and indicates Pirzada's significantly more complex trust model is actually less effective.

Packet Throughput Results: Figure 2

Packet throughput is directly comparable to the amount of data that can be transmitted between a source and destination, with Trusted AODV showing a clear advantage over AODV. This is because AODV is easily fooled and thus, one malicious node can easy intercept a lot of packets, causing the instantaneous drop to 50% throughput as soon as one malicious node is present.

Average Number of Hops: Figure 3

The average number of hops is clearly related to latency and throughput and shows that Trusted AODV is able to sustain longer routes with a higher proportion of malicious nodes. This means that a greater distance can be covered by the network successfully.

Packet Overhead: Figure 4

The increased performance of Trusted AODV does come at a cost as the packet overhead indicates, where packet overhead is the proportion of control packets compared to number of data packets. The proportion of control packets sent is significantly greater for Trusted AODV, due to the continual modification of the network topology caused by the trusted protocol removing malicious nodes from the network. Although it is a large overhead, the performance gain is significant and with more research the overhead can be reduced. It is always preferable to have a functioning network at the expense of more control packets, than a dysfunctional network with minimal control packets.

Overall it is clear that even a basic trust model has clear advantages and Trusted AODV is showing significantly more promising results than A. A. Pirzada.

Conclusion

Overall the project has been a success and has achieved its initial aims. We have shown that trust can play an important role in an ad hoc network, the results produced by Pirzada have been explained and the ground work for further research in ad hoc networks within the department has been done. The project has not gone as far as was initially hoped, due to time and difficulties with NS-2. Although a lot more than just research has been achieved, as to get these results a lot of dead ends have been travelled and a lot of data manipulation and configuration scripts created. This will allow anyone continuing after us, not to follow in our footsteps but to walk on from where we stand, providing a perfect platform for further research.

My Experience

I found the project to be very challenging throughout, a bit of an upward struggle at times. This was mainly due to starting the project from scratch, as we were the first people to research ad hoc networking within the department of Computer Science. This meant that setup, configuration and implementation took a significant amount of time before useful results could be generated. This was obviously meaningful work but meant that the progress of research was very slow. Although, on a positive note the time spent has not been wasted and will allow for our successors to progress much more quickly with their research.

I have enjoyed the experience and found the working atmosphere within Computer Science pleasant and would like to thank my supervisor for being very helpful. I have discovered although pure research is not the career I intend to take, the prospect of a job with research and development is appealing, which without URSS I may not have discovered.

References

[1] A.A. Pirzada and C. McDonald. Establishing trust in pure ad-hoc networks.
in: Proceedings of the 27th Australasian Computer Science Conference (ACSC), vol. 26, no. 1, 2004, pp. 47-54.
[2] A. A. Pirzada, A. Datta and C. McDonald. Incorporating trust and reputation in the DSR protocol for dependable routing,
Computer Communications, Vol. 29, pp. 2806-2821, 2006.
[3] A. A. Pirzada and C. McDonald. Trust Establishment in Pure Ad-Hoc Networks.
Wireless Personal Communications, Vol. 37(1-2), pages 139-168, 2006.

Project by: **Anthony Dawson**
Supervisor: **Nathan Griffiths**

THE UNIVERSITY OF WARWICK