Security Vulnerabilities in Ad Hoc Networks*

Po-Wah Yau and Chris J. Mitchell
Mobile VCE Research Group
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
P.Yau@rhul.ac.uk, C.Mitchell@rhul.ac.uk

ABSTRACT

Mobile ad hoc networks have inherently different properties than traditional wired networks. These new characteristics present different security vulnerabilities and this paper provides a detailed classification of these threats. Threats exist to a mobile ad hoc network both from external nodes unauthorised to participate in the mobile ad hoc networks, and from internal nodes, which have the authorisation credentials to participate in the mobile ad hoc network. Internal nodes giving rise to threats can be further divided according to their behaviour — failed, badly failed, selfish and malicious nodes. Failed and selfish nodes are those which do not perform certain operations that the protocol specifies that they should, the former due to some unforeseen failure and the latter due to selfishness to conserve power. Badly failed nodes may perform operations incorrectly, introducing false and misleading information into the network. Malicious nodes may deliberately disrupt the network using a variety of attacks. All categories of node behaviour should be considered when designing protocols for mobile ad hoc networks.

1. INTRODUCTION

Mobile ad hoc networks have inherently very different properties than conventional networks. A lack of infrastructure presents problems with centrally controlled security, for example access control, which is traditionally maintained by a central server. Also, security mechanisms involving trusted third parties may no longer be viable in ad hoc networks. As nodes may be mobile, entering and leaving the network, a dynamic topology means that security will have to be scalable. Communication is likely to be wireless, so bandwidth will be limited. An even more important constraint is energy. This introduces issues with heterogenous networking, where resource intensive security mechanisms may not work in an ad hoc environment.

This paper concentrates on presenting a general threat model for mobile ad hoc networks which classifies the different behaviours of mobile ad hoc nodes into external threats by unauthorized entities, and internal threats posed by trusted entities. One of the key research areas in mobile ad hoc networks is setting up and maintaining the ad hoc infrastructure through the use of routing protocols. Existing protocols are likely to be too resource intensive to be suitable for ad hoc network use, so many solutions using a variety of different methods are currently the subject of ongoing research. This paper will use routing protocols as an example to demonstrate the threat model.

Section 2 covers the terminology used. Section 3 gives generic descriptions of the different types of routing protocols that have been proposed. Section 4 describes the threat model, after defining some general security requirements. Sections 5 and 6 classify the possible external and internal threats. Finally, section 7 comments on scenarios for simulations of mobile ad hoc networks.

2. TERMINOLOGY

The following terms are used in this document, but may be used differently elsewhere. A *node* is a device with a network interface that is participating in routing in a mobile ad hoc network. It may or may not be mobile, and may also be part of another network. It is important to realise that a node can actually be a large network, or it could be just a single mobile device such as a mobile phone. An *originator node* is a node which originates a data packet, intended for a certain *destination node*. A node is a *neighbour node* of another node if it is only one hop away and within direct transmission range. If the destination node is not a neighbour node of the originator node, the data packet will have to traverse a multi-hop route consisting of *intermediate nodes*. In a specific scenario, the *sending node* is the last node to have forwarded the data packet. A *routing packet* is any packet used by a routing protocol to affect routing information. Examples include routing updates, periodic neighbour beacons, route requests, route replies and route error messages. *Route request, reply* and *error* packets are used in reactive protocols. See Section 3 for details of how these routing packets are used.

A *Source route/Route record* is a sequential list of node addresses from the originator node to the destination node, and is used in the Dynamic Source Routing protocol (DSR) [9, p140]. In the context of sending data packets along a route, the *Forward Path* is the (downstream) route from originator node to destination node. Conversely, the *Reverse Path* is the (upstream) route from the destination to originator node.

*The work reported in this paper has formed part of the Networks & Services area of the Core 2 Research Programme of the Virtual Centre of Excellence in Mobile & Personal Communications, Mobile VCE, www.mobilevce.com, whose funding support, including that of EPSRC, is gratefully acknowledged. Fully detailed technical reports on this research are available to Industrial Members of Mobile VCE

3. MOBILE AD HOC ROUTING

Routing is a major area of research in ad hoc networks, as the characteristics of ad hoc networks pose many new challenges by comparison with traditional wired area networks. Existing protocols are likely to be too resource intensive to be suitable for ad hoc use, so many solutions using a variety of methods are being proposed and studied. The Internet Engineering Task Force (IETF) has set up a working group called MANET[1], with the objective of selecting the most suitable protocols[2]. There are two main types of ad hoc network routing protocols, pro-active and reactive protocols. Within these categories, different implementations use a variety of techniques to find and maintain routes. Most routing protocols are table-driven, where information is processed and stored in routing tables, but other novel methods have been proposed.

Reactive protocol operation is typically divided into a route discovery cycle and route maintenance. A node initiates route discovery when it needs to send a data packet to a destination whose route is unknown. This typically involves broadcasting some form of route request message, where an intermediate or the destination node itself can provide the originator node with a reply, containing the route to the destination. Route maintenance is required as there are no periodic route update messages. Instead, when a link break is detected between two nodes, one or both nodes are responsible for propagating error information about the broken link to all affected parties. Examples of reactive routing schemes are the Ad hoc On-Demand Distance Vector (AODV)[3] protocol [12]; Dynamic Source Routing (DSR)[3] [9], which uses 'source routes' and finally, Location Aided Routing (LAR) [14] which is a location assisted protocol, using geographical coordinates to increase the efficiency of routing.

Pro-active protocols use periodic topology updates to disseminate route information throughout the whole network, but try to minimise the information being sent in order to save bandwidth. Various techniques are used to achieve this, as exemplified by Optimised Link State Routing (OLSR) [3] and Topology Broadcast Reverse Path Forwarding (TBRFP)[3] [1].

Hybrid routing protocols use both pro and reactive techniques to control a hierarchical architecture. The Zone Routing Protocol ZRP[3] [5, 6] is a hybrid protocol which actually combines three sub-protocols — the Interzone Routing Protocol (IERP)[3], the Intrazone Routing Protocol (IARP)[3] and the Broadcast Resolution Protocol (BRP)[2].

Other hierarchical protocols have been proposed which function on top of another routing protocol. Both Fisheye State Routing (FSR)[3] [11] and Landmark Routing (LANMAR)[3] [4] attempt to introduce optimisations by organising an implicit hierarchy on top of a proactive routing protocol.

4. THE ROUTING THREAT MODEL

[1] `http://www.ietf.org/html.charters/manet-charter`

[2] The current IETF Internet-Drafts of MANET routing protocols can be found at `http://www.ietf.org/ids.by.wg/manet.html`

[3] Currently being considered for adoption as an IETF standard

This section describes the threat model for ad hoc networks. Section 4.1 defines the security services which are covered in the threat model, before sections 5 and 6 elaborate on how ad hoc nodes can behave.

4.1 Ad Hoc Network Routing Threats

The main threats to an ad hoc network routing protocol are as follows. This list also provides the basis for a generic list of security requirements.

- *Confidentiality.* The primary confidentiality threat in the context of routing protocols is to the privacy of the routing information itself, which leads to a secondary privacy threat to information such as the network topology, geographical location, etc.

- *Integrity.* The integrity of a network depends on all nodes in the network following correct routing procedures so that every node has correct routing information. Therefore threats to integrity are those which either introduce incorrect routing information or alter existing information.

- *Availability.* This is defined as access to routing information at all times upon demand. If a route exists to a mobile node, then any node should be able to get that route when they require it. Also a routing operation should not take an excessive amount of time to perform, delaying a node from receiving up-to-date route information. Related to this, a node should be able to carry out normal operations without excessive interference caused by the routing protocol or security.

- *Authorisation.* An unauthorised node is one which is not allowed to have access to routing information, and is not authorised to participate in the ad hoc routing protocol. There is no assumption that there is an explicit and formal protocol, simply an abstract notion of authorisation. However, as discussed below, formal identity authentication is a very important security requirement, needed to provide access control services within the ad hoc network.

- *Dependability and reliability.* One of the most common applications for ad hoc networks is in emergency situations when the use of wired infrastructure is infeasible. Hence, routing must be reliable, and emergency procedures may be required. For example, if a routing table becomes full due to memory constraints, a reactive protocol should still be able to find an emergency route to a given destination.

- *Accountability.* This will be required so that any actions affecting security can be selectively logged and protected, allowing for appropriate reaction against attacks. As explained below, the misbehaviours demonstrated by different types of nodes will need to be detected, if not prevented. Event logging will also help provide non-repudiation, preventing a node from repudiating involvement in a security violation.

4.2 Internal and External Threats

The threat model used here distinguishes between external and internal attacks — see also [16, p.25]. External attacks are performed by unauthorised nodes or entities. These threats are likely to be more easily detected than threats from internal nodes. Internal attacks are posed by internal nodes, i.e. they are performed by authorised nodes within the ad hoc network. These threats are thus likely to be more difficult to detect as they arise from trusted sources.

In the text below, 'correct' data packets and 'correct' procedures are simply those that adhere strictly to the routing protocol being used. By contrast 'incorrect' data packets and 'incorrect' procedures are those which are in any way different to the format and behaviour as stated in the protocol. 'False' data packets are data packets that are of the correct protocol format, but contain false information.

5. EXTERNAL THREATS

In the presence of an authentication protocol to protect the upper layers, external threats are directed at the physical and data link layers. Physical layer security is intrinsically difficult to provide due to the possibly mobile nature of ad hoc nodes.

We divide external threats into two major categories: *passive eavesdropping*, where the adversary simply listens to transmitted signals, and *active interference*, where the opponent sends signals or data designed to disrupt the network in some way.

5.0.1 Passive eavesdropping

This can allow unauthorised principals to listen to and receive messages including routing updates. An unauthorised node will be able to gather data that can be used to infer the network topology, and other information such as the identities of the more heavily used nodes which forward or receive data. Hence, techniques may be needed to hide such information. Eavesdropping is also a threat to location privacy. Note that passive eavesdropping also allows unauthorised nodes to discover that a network actually exists within a geographical location, by just detecting that there is a signal present. Traffic engineering techniques have been developed to combat this.

5.0.2 Active Interference

The major threat from active interference is a denial of service attack caused by blocking the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and the routing protocol in use. With regard to the routing of data packets, reactive routing protocols may see a denial of service attack as a link break. Route maintenance operations will cause most protocols to report the link as broken so that participating nodes can find an alternative route. Proactive routing protocols do not react immediately to non-delivery of data packets. If the route is believed to be broken, it will eventually be timed out and deleted.

Probably the most serious type of denial of service attack is a sleep deprivation torture attack [13, p4], where node energy is deliberately wasted. With limited power and resources, prevention of such attacks is of utmost importance. Security against such attacks has already been extensively studied and developed by the military for packet radio networks. Spread spectrum technology is designed to be resistant to noise, interference, jamming, and unauthorized intrusion [7].

It is prudent to note that protection against sleep deprivation torture cannot be achieved at the physical layer, even though power constraint is indeed a physical layer attribute. The fact that power levels affect all ad hoc network operations makes securing such networks particularly difficult.

There are also threats to integrity, e.g. where an external attacker can attempt to replay old messages, or change the order of messages. Old messages may be replayed to reintroduce out-of-date information. Out-of-date routing information could lead to further denial of service attacks as nodes try to use old but invalid routes, or delete current valid routes. If the routing protocol utilises neighbour sensing by monitoring received data packets, replaying old packets may falsely lead nodes into believing that an 'old' link with a neighbour has become active and usable again.

6. INTERNAL THREATS

The threats posed by internal nodes are very serious, as internal nodes will have the necessary information to participate in distributed operations. Internal nodes can misbehave in a variety of different ways; we identify four categories of misbehaviour — failed nodes, badly failed nodes, selfish nodes and malicious nodes.

Note that two misbehaving nodes within the same category may exhibit different degrees of incorrect node behaviour. For example, some nodes will be more selfish than others. Also, a node may demonstrate behaviours from more than one category — indeed, this may even be the typical case.

6.1 Failed Nodes

Failed nodes are simply those unable to perform an operation; this could be for many reasons, including power failure and environmental events. The main issues for ad hoc routing are failing to update data structures, or the failure to send or forward data packets, including routing messages. This is important as those data packets may contain important information pertaining to security, such as authentication data and routing information. A failure to forward route error messages will mean that originator nodes will not learn of broken links and continue to try to use them, creating bottlenecks. The threat of having failed nodes is most serious if failed nodes are needed as part of an emergency route, or form part of a secure route.

6.2 Badly Failed Nodes

Badly failed nodes exhibit features of failed nodes such as not sending or forwarding data packets or route messages. In addition they can also send false routing messages, which are still correctly formatted, but which contain false information and are a threat to the integrity of the network. For example, false route requests for a node which does not exist may circulate in the ad hoc network using up valuable bandwidth, as no

node can provide a suitable reply. Unnecessary route requests for routes which badly failed nodes already have, might also be sent. False route replies in response to a true route request may result in false routes being set up and being propagated through the network. False route error messages will cause working links to be marked as broken, potentially initiating a route maintenance procedure.

Protocols which rely on neighbour sensing operations are also vulnerable, as false messages may cause nodes to 'sense' extra neighbours. This is especially true in protocols such as LANMAR, which do not rely on a specific neighbour sensing message, but if a routing control message is received directly which contains an unknown source address, then that address is used as a new neighbour [4, p2].

Protocols such as AODV include within the route error messages a list of affected nodes to which the route errors should be unicast [12, p211]. If this list is large, then the threat not only affects network integrity, but is also a denial of service attack, as resources and bandwidth are being used up by the large volume of route error messages sent, and the unnecessary route requests and replies used to find alternative routes.

6.3 Selfish Nodes

Selfish nodes exploit the routing protocol to their own advantage, e.g. to enhance performance or save resources. Selfish nodes are typified by their unwillingness to cooperate as the protocol requires whenever there is a personal cost involved, and will exhibit the same behaviours as failed nodes, depending on what operations they decide not to perform. Packet dropping is the main attack by selfish nodes, where most routing protocols have no mechanism to detect whether data packets have been forwarded, DSR being the only exception [9]. Thus, another pattern of behaviour to consider is partial dropping, which could be difficult to prevent and detect. It is important to emphasise that, in this model, selfish nodes do not perform any action to compromise network integrity by actively introducing incorrect information.

6.4 Malicious Nodes

Malicious nodes aim to deliberately disrupt the correct operation of the routing protocol, denying network services if possible. Hence, they may display any of the behaviours shown by the other types of failed nodes. The impact of a malicious node's actions is greatly increased if it is the only link between groups of neighbouring nodes.

6.4.1 Denial of Service Attacks

The most common threats lead to a denial of service attack, which in turn induces the 'sleep deprivation torture' attack [13, p4]. Malicious nodes cause other nodes to exhaust their resources by getting other mobile nodes to do unnecessary processing using correct or incorrect information. Those nodes which use up their power resources will eventually become unable to operate under normal circumstances. A sleep deprivation torture attack is particularly viable for ad hoc networks, due to the power constraints likely for mobile nodes. There are a variety of ways to achieve the objective of this denial of service attack. For example, in proactive protocols a malicious node could advertise topology updates with lots of false routes and addresses so that the route table calculation will take more time and resource. This is also an attack on network integrity.

6.4.2 Attacks on Network Integrity

Many denial of service attacks are also threats to network integrity, exploiting the routing protocol to introduce incorrect routing information. Another factor is that the more densely populated is the area in which a malicious node attacks, the more nodes will be affected. Protocols such as OLSR use a pure flooding mechanism so false information will be relayed to every node [3, p4]. With the hierarchical FSR protocol, participating nodes far away from the malicious node will be less sensitive to its injected false information, especially in a multi-scope implementation [11, p2]. Hence, the preferred environment for a malicious node in a FSR controlled network is to have few scopes of a large size, to make sure false information is periodically broadcast as often and to as many nodes as possible.

6.4.3 Attacking Neighbour Sensing Protocols

Malicious nodes can either force nodes to incorrectly add neighbours when they do not exist, or cause nodes to ignore valid neighbour nodes. The method will depend on the neighbour sensing protocol but most require the receipt of some form of message. As with a badly failed node, a malicious node can send a neighbour sensing message with a false source address to cause the same effects.

For a malicious node to cause another node to ignore its neighbours, it could perform an active denial of service attack similar to external nodes. However, this could also be easily detected. Thus, this attack will be more successful for the malicious node if it could exploit some other operation such as a blacklist. If a bi-directional MAC[4] protocol is in use, DSR uses a blacklist for neighbours a node believes it has asymmetrical links with [9]. Thus, a malicious node could just try to block transmission in one direction to cause the node to be added to its blacklist. Blacklisted entries either expire or are deleted when bi-directional communication has been confirmed. So, conversely, a malicious node could try to force a node to delete neighbours from its blacklist by masquerading as a blacklisted node, and forward a route request, whose source header contains details of the blacklisted node (its IP address etc.). A similar attack can be achieved with AODV [12].

6.4.4 Misdirecting Traffic

As previously mentioned, a malicious node can usually masquerade by just using a false source address in the data packets it sends, as described in FSR [11]. In FSR, nodes examine the IP Header source address and use it as a neighbour address. If the malicious node uses a false address which belongs to another node, then it can affect network integrity by getting all nodes in the network to point their routes to the malicious node, instead of the true owner of the source address. A malicious node can do this in a reactive protocol by reply-

[4]Medium Access Control

ing to route requests before the original owner can, and the same effect can be achieved in a proactive protocol where the malicious node just advertises false routes in the hope they get accepted before the true routes. The malicious node will then receive any information which was intended for the owner of the address. This attack has been named the 'black hole' attack [10, p4], akin to the celestial structure which sucks in all objects and matter.

Another reason for masquerading in this way is when the malicious node targets another node and cause excess traffic to be routed to it, causing a targeted sleep deprivation attack. A malicious node could send false route requests on behalf of this node, so that other nodes will then direct route replies to the node. Malicious nodes can advertise routes with attractive route metrics and high sequence number so that the likelihood of the false route being accepted is increased. However, the further away a malicious node is, the less successful this attack will be in getting the false routes accepted before the true routes.

However, as identified and addressed by [8, p2], another attack exists to cause a similar effect. In the 'Wormhole' attack, a malicious node tunnels packets. In a reactive routing network, tunnelling route requests close to the destination node will result in the tunnelled route being replied to, and all other route requests being ignored. Thus the malicious node has injected itself into the route. In a proactive routing network, the same technique can be used to tunnel neighbour sensing messages, in order to attack neighbour sensing protocols as described above.

6.4.5 *Exploiting Route Maintenance*

Malicious nodes can simply propagate false route error messages so that valid working links are marked as broken. Resources will be used in attempts to repair the links or find alternative routes. An alternative attack may be for a malicious node to coerce another node into sending route error messages by blocking an operational link (e.g. by blocking acknowledgments in DSR [9, p147]). This attack can also be performed by an external attacker.

6.4.6 *Attacking Sequence Numbers and Duplicate Mechanism*

Unique sequence numbers prevent replay attacks of old data packets. However, this mechanism can also be exploited to cause a denial of service. A malicious node could flood the network with as many messages with false source addresses containing as many high sequence numbers as possible. Thus any true messages sent will be discarded as duplicated or out of sequence. This attack is possible because most protocols require nodes to maintain their own sequence number counter, and do not take into account the sequence numbers of received messages. Note that this discussion refers to message identifier sequence numbers and not the sequence numbers used to guarantee route freshness as in AODV and OLSR.

6.4.7 *Attacks on Protocol Specific Optimisations*

There are many protocol specific attacks. The following describes an attack on the DSR salvaging operation which is used to find alternative routes when a link break is detected [9, p151].

Using the attacks just described above, the malicious node injects into the network as many routes, with as many different next hops, as possible, all of which do not exist and all point to the same target. The malicious node then sends a data packet addressed for that non-existent target. This is a denial of service attack as an intermediate node will now attempt to send route error messages for each next-hop from which it tries to gain an acknowledgement. The intermediate node then tries to salvage the data packet by finding an alternative route. The alternative route is likely to be another false route and this carries on until the data packet has been the subject of MAX_SALVAGE_TIMES salvage attempts. Of course the malicious node can just send a data packet for the same target to repeat the denial of service.

7. PROTOCOL, MECHANISM AND SIMULATION DESIGN ISSUES

A motivation for this threat model is to produce more realistic scenarios and simulations, in order to properly test security mechanisms designed to cope with all the different types of node behaviour, producing feasible solutions which will work in a real and practical system. Early simulations of ad hoc networks have often been too 'clean' or 'vanilla' where the system runs too smoothly and uniformly. Network topology has a major impact on the effect of the realisation of threats. Thus the following properties affect the possible threats identified in the threat model, and should be considered when designing secure protocols and simulation studies to test such protocols.

- *Size.* It is a prerequisite that the network size should be changeable. Indeed, size should be made a dynamic variable which changes as nodes enter and leave the ad hoc network. Simulations should ideally also cover the case where large numbers of nodes simultaneously enter or leave the network.
- *Density of nodes.* Denial of service threats will be more difficult to achieve in crowded than sparsely populated areas. The simple reason is that the more nodes there are, the more possible alternative routes exist. However, threats to network integrity may be more serious in dense areas as any false information will propagate faster.
- *Position of nodes.* This describes the problem of nodes which drift in and out of transmission range of the ad hoc network at the perimeter, and also any partitioning where only a few nodes link two groups of nodes. Here the perimeter of the network may be the actual physical perimeter, or the logical perimeter of a collection of network nodes which are cooperating with each other. Denial of service threats are more serious here, as boundary nodes will have fewer routes to the rest of the ad hoc network. In both scenarios, there are fewer routes to attack to perform a successful a denial of service attack.
- *Grouping.* Allied to the position of nodes should be some means of simulating the grouping of nodes.

The property of locality of reference refers to the fact that nodes will communicate with a common group of nodes, often those closest to it. In any case, scalability will probably see ad hoc routing using some form of hierarchical model, as with the Internet. Grouping may be temporary with a high number of nodes leaving and joining (e.g. a hotspot location), or quite permanent (e.g. a Personal Area Network).

- *Mobility.* It has to be emphasised that not all ad hoc nodes have to be mobile. Therefore, protocols and their simulations should include stationary nodes. In terms of practicality, research may reveal that ad hoc networks may not be able to function without some semi-central entities anyway. Thus the number of stationary nodes should be an automatically dynamic variable. When simulating mobile nodes, care must be taken to make their movement random [15]. Their speed should not be constant and their movement made of different curves and lines. Elucidating the previous design point, groups of nodes will also move together, for example nodes in a car. Since some nodes may move very quickly, protocols will have to cope with nodes entering and leaving at a high rate. For example, nodes belonging to people and shops in a street may want to network together and share services as they know there will be some link persistence. They may however, wish to ignore nodes in a car which drives past as the relationship will not be long-lasting enough for any practical benefit to result.

- *Relationships.* Most current simulations include a node randomly sending another node a data packet or route request. Although this may be too complicated to implement, simulations should ideally include relationships of differing length. Short term relationships of seconds and long term relationships of many minutes should both be covered. The motivation for this arises from recent reputation research [2]. The differing lengths of relationships can dictate how good or bad reputations will be considered and managed.

8. CONCLUSION

Mobile ad hoc networks present different threats due to their very different properties. These properties open up very different security risks from conventional wired networks, and each of them affects how security is provided and maintained. All four types of internal threat identified above give rise to different security requirements, several of which apply to ad hoc routing. Any protocols and simulations to test them should include the capability to handle each type of node and attack.

9. REFERENCES

[1] B. Bellur and R. Ogier. A reliable, efficient topology broadcast protocol for dynamic networks. In *Proceedings IEEE INFOCOM '99, The Conference on Computer Communications, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, The Future Is Now, 21-25 March, 1999, New York, NY, USA*, volume 1, pages 178–186. Institute of Electrical and Electronics Engineers, IEEE Press, 1999.

[2] S. Buchegger and J-Y. Le Boudec. Performance analysis of the CONFIDANT protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks). In J. Hubaux, J. J. Garcia-Luna-Aceves, and D. Johnson, editors, *Proceedings of The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing, 9-11 June, 2002, Lausanne, Switzerland*, 238, pages 226–236. Association for Computing Machinery, ACM Press, 2002.

[3] T. Clausen, G. Hansen, L. Christensen, and G. Behrmann. The optimized link state routing protocol, evaluation through experiments and simulation. In *Proceedings 4th International Symposium on Wireless Personal Multimedia Communications, September 9-12, 2001, Aalborg, Denmark*, pages 841–846. Institute of Electrical and Electronics Engineers, IEEE Press, 2001.

[4] M. Gerla, X. Hong, and G. Pei. LANMAR: landmark routing for large scale wireless ad hoc networks with group mobility. In N. Vaidya, M. Corson, and S. Das, editors, *Proceedings of the first ACM international symposium on Mobile and ad hoc networking and computing, August 11, 2000, Boston, Massachusetts, USA*, 150, pages 11–18. Association for Computing Machinery, ACM Press, 2000.

[5] Z. Haas and M. Pearlman. The performance of query control schemes for the zone routing protocol. In A. Sen and N. Vaidya, editors, *Proceedings of the 3rd international workshop on Discrete algorithms and methods for mobile computing and communications, September 2, 1999, Seattle, Washington, USA*, 92, pages 23–29. Association for Computing Machinery, ACM Press, 1999.

[6] Z. Haas and M. Pearlman. ZRP a hybrid framework for routing in ad hoc networks. In C. Perkins, editor, *Ad Hoc Networking*, chapter 7, pages 221–253. Addison-Wesley, 2001.

[7] A. Hassan, W. Stark, and J. Hershey. Frequency-hopped spread spectrum in the presence of a follower partial-band jammer. *IEEE Transactions on Communications*, 41(7):1125–1131, 1993.

[8] Y. Hu, A. Perrig, and D. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In *To be published in Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, April 1-3, 2003, San Fransisco, CA, USA*. Institute of Electrical and Electronics Engineers, IEEE Press, 2003.

[9] D. Johnson, D. Maltz, and J. Broch. DSR the dynamic source routing protocol for multihop wireless ad hoc networks. In C. Perkins, editor, *Ad Hoc Networking*, chapter 5, pages 139–172. Addison-Wesley, 2001.

[10] J. Lundberg. Routing security in ad hoc networks. In Heidi Pehu-Lehtonen Helger Lipmaa, editor, *Proceedings of the Helsinki University of Technology Seminar on Network Security, Fall 2000, Helsinki, Finland*. Helsinki University of Technology, 2000. Proceedings are only available online at http://www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers/.

[11] G. Pei, M. Gerla, and T-W. Chen. Fisheye state routing: A routing scheme for ad hoc wireless networks. In *2000 IEEE International Conference on Communications, ICC 2000, Global Convergence Through Communications, June 18-22, 2000, New Orleans, USA*, volume 1, pages 70–74. Institute of Electrical and Electronics Engineers, IEEE Press, 2000.

[12] C. Perkins and E. Royer. The ad hoc on-demand distance-vector protocol. In C. Perkins, editor, *Ad Hoc Networking*, chapter 6, pages 173–219. Addison-Wesley, 2001.

[13] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In B. Christianson, B. Crispo, and M. Roe, editors, *Security Protocols, 7th International Workshop, April 19-21, 1999, Cambridge, UK*, volume 1796 of *Lecture Notes in Computer Science*, pages 172–194. Springer, 2000.

[14] Y. Tseng, S. Wu, W. Laio, and C. Chao. Location awareness in ad hoc wireless mobile networks. *IEEE Computer*, 34(6):46–52, June 2001.

[15] J. Yoon, M. Liu, and B. Noble. Random waypoint considered harmful. In *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, April 1-3, 2003, San Fransisco, CA, USA*. Institute of Electrical and Electronics Engineers, IEEE Press, To appear.

[16] L. Zhou and Z. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, November 1999.