International Journal of Research in Science And Technology http://www.ijrst.com
(IJRST) 2012, Vol. No. 2, Issue No. II, Apr-Jun **ISSN: 2249-0604**

ON DEMAND ROUTING PROTOCOLS IN MOBILE NETWORK

Madhu Malik

ABSTRACT

Mobile Network assume no pre-deployed infrastructure is available for routing packets end-to-end in a network, and instead rely on intermediary peers. Securing ad hoc routing presents challenges because each user brings to the network their own mobile unit, without the centralized policy or control of a traditional network. Especially, Security flaws of routing protocol may cause severe problems under ad hoc network. In this paper we briefly present the most popular on-demand routing protocol ADOV and potential security problems of AODV. Then, this paper analyzes security requirements for ad hoc routing protocols and proposed solutions such as ARAN, SAODV, SAR and SRP.

INTRODUCTION

A **mobile network** (**MANET**), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Securing ad hoc routing presents another challenge because each user brings to the network their own mobile unit, without the centralized policy or control of a traditional network.

Ad hoc network routing protocols are challenging to design, and secure ones are even more so. Wired network routing protocols do not handle well the type of rapid node mobility and network topology changes that occur in ad hoc networks; such protocols also have high communication overhead because they send periodic routing messages even when the network is not changing. So far, researchers in ad hoc networking have generally studied the routing problem in a non-adversarial network setting, assuming a trusted environment; relatively little research has been done in a more realistic setting in which an adversary may attempt to disrupt the communication.

We focus here on *on-demand* (or reactive) routing protocol for ad hoc networks, in which a node attempts to discover a route to some destination only when it has a packet to send to that destination. On-demand routing protocols have been demonstrated to perform better with significantly lower overheads than periodic (or proactive) routing protocols in many situations, since they are able to react quickly to the many changes that may occur in node connectivity, yet are able to reduce (or eliminate) routing overhead in periods or areas of the network in which changes are less frequent.

The following section presents related work in securing the routing protocols. Section 3 presents a brief introduction to the ad hoc routing protocol AODV. Section 4 presents the possible attacks that a malicious node can use for disrupting the operation of a routing protocol in a self-organized network. In Section 5 we describe security requirements of ad hoc networks and in section 6 we analyze the already proposed secure ad hoc routing protocols that exist in the literature and present their operational principles.

RELATED WORK

Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad hoc networks and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins and S. Das. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand [1]. Traditional ad hoc routing protocols do not provide any security therefore secure routing in MANETs has been of interest for quite long time in the research community. In this section we will give a short overview of existing work and entry points to the literature.

Zhou and Haas [2] primarily discuss key management. They devote a section to secure routing, but essentially conclude that "nodes can protect routing information in the same way they protect data traffic". They also observe that denial-of-service attacks against routing will be treated as damage and routed around.

Some work has been done by S. Marti, T. J. Giuli [3] to secure ad hoc networks by using misbehavior detection schemes. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving (especially because it is very hard to distinguish misbehaving from transmission failures and other kind of failures); and second, it has no real means to guarantee the integrity and authentication of the routing messages.

Kimaya Sanzgiri et al [4] proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN, every node that forwards a route discovery or a route reply message must also sign it, (which is very computing power consuming and causes the size of the routing messages to increase at each hop), whereas the proposal presented in this paper only require originators to sign the message. In addition, it is prone to reply attacks using error messages unless the nodes have time synchronization.

Hubaux, et al. have proposed a method that is designed to ensure equal participation among members of the ad hoc group, and that gives each node the authority to issue certificates [5]. Kong, et al. [6] have proposed a secure ad hoc routing protocol based on secret sharing; unfortunately, this protocol is based on erroneous assumptions, e.g., that each node cannot impersonate the MAC address of multiple other nodes. Yi, et al. [7] also have proposed a general framework for secure ad hoc routing called the SAR.

Papadimitratos and Haas [8] proposed a protocol (SRP) that can be applied to several existing routing protocols. SRP requires that, for every route discovery, source and destination must have a

security association between them. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected, and any malicious node can just forge error messages with other nodes as source. Securing the AODV protocol has been made by Zapata with his SAODV [9]. This is the background of secure routing protocols for the AODV routing protocol. In this paper I review all these routing protocols.

AD HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV)

Routing protocols in mobile networks are subdivided into two basic classes:
• Proactive routing protocols
• Reactive routing protocols
The proactive routing protocols (e.g. OLSR) are table-driven. They usually use link-state routing algorithms flooding the link information. Link-state algorithms maintain a full or partial copy of the network topology and costs for all known links. The reactive routing protocols (e.g. AODV) create and maintain routes only if these are needed, on demand. They usually use distance-vector routing algorithms that keep only information about next hops to adjacent neighbors and costs for paths to all known destinations. Thus, link-state routing algorithms are more reliable, less bandwidth-intensive, but also more complex and compute- and memory-intensive.
An alternative approach to the one followed by table-driven protocols is the source-initiated on-demand routing. According to this approach a route is created only when the source node requires one to a specific destination. A route is acquired by the initiation of a *route discovery* function by the source node. The data packets transmitted while a route discovery is in process are buffered and are sent when the path is established. An established route is maintained as long as it is required through a *route maintenance* procedure. The Ad hoc On-demand Distance Vector (AODV) routing protocol and the Dynamic Source Routing protocol are examples of this category of protocols also known as *reactive*.

AODV is a relative of the Bellmann-Ford distant vector algorithm, but is adapted to work in a mobile environment. AODV determines a route to a destination only when a node wants to send a packet to that destination. Routes are maintained as long as they are needed by the source. Sequence numbers ensure the freshness of routes and guarantee the loop-free routing.

Merits of AODV
The AODV routing protocol does not need any central administrative system to control the routing process. Reactive protocols like AODV tend to reduce the control traffic messages overhead at the cost of increased latency in finding new routes. AODV reacts relatively fast to the topological changes in the network and updates only the nodes affected by these changes. The HELLO messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network. The AODV routing protocol saves storage place as well as energy. The destination node replies only once to the first request and ignores the rest. The routing table

maintains at most one entry per destination. If a node has to choose between two routes, the up-to-date route with a greater destination sequence number is always chosen. If routing table entry is not used recently, the entry is expired. A not valid route is deleted: the error packets reach all nodes using a failed link on its route to any destination.

Drawbacks of AODV

It is possible that a valid route is expired. Determining of a reasonable expiry time is difficult, because the nodes are mobile, and sources' sending rates may differ widely and can change dynamically from node to node. Moreover, AODV can gather only a very limited amount of routing information; route learning is limited only to the source of any routing packets being forwarded. This causes AODV to rely on a route discovery flood more often, which may carry significant network overhead. Uncontrolled flooding generates many redundant transmissions which may cause so-called broadcast storm problem. The performance of the AODV protocol without any misbehaving nodes is poor in larger networks. The main difference between small and large networks is the average path length. A long path is more vulnerable to link breakages and requires high control overhead for its maintenance. Furthermore, as a size of a network grows, various performance metrics begin decreasing because of increasing administrative work, so-called administrative load. AODV is vulnerable to various kinds of attacks, because it based on the assumption that all nodes will cooperate. Without this cooperation no route can be established and no packet can be forwarded. There are two main types of uncooperative nodes: malicious and selfish. Malicious nodes are either faulty and cannot follow the protocol, or are intentionally malicious and try to attack the network. Selfishness is no cooperation in certain network operations, f.e. dropping of packets which may affect the performance, but can save the battery power.

EXPLOITS ALLOWED BY EXISTING PROTOCOLS

In the wired environment, the routing protocols are based on trust relationship of two participating nodes when exchanging routing information since a lot of routers in the Internet usually have been operated by trustworthy companies. Current ad hoc routing protocols also inherently trust all participants because most of them are based on the routing protocols of wired networks. Thus, most ad hoc routing protocols are cooperative and depend on neighboring nodes to route packets. However, this naïve trust model allows a malicious attacker to paralyze an entire ad hoc network by easy way, such as inserting erroneous routing information. To achieve availability of ad hoc networks, routing protocols should be robust against this kind of malicious attacks. Then, let's look at the common security threats in ad hoc routing protocols. There are two sources of attacks to routing protocols. The first one is done by external attackers. For example, by injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excessive traffic load into the network by causing retransmission and in efficient routing. The second one, which is more severe, is done

by compromised nodes, which might advertise incorrect routing information to other nodes. Under this attack, Detection of such incorrect information and compromised node is very difficult.
We can also classify the attacks into passive and active ones.

Passive attack

It means that the attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routing traffic. The major advantage for the attacker in passive attacks is that in a wireless environment the attack is usually impossible to detect. Furthermore, routing information can reveal relationships between nodes; disclose their IP addresses, or even the network topology. If a route to a particular node is requested more often than to other nodes, the attacker might expect that the node is important for the functioning of the network, and can decide that node as a victim of his attack, which might bring the entire network down.

Active attack

Besides the passive attack, this active attack is performed by the attacker who can inject arbitrary packets into the network. The goal may be to attract packets destined to other nodes to the attacker for analysis or just to disable the network. A major difference in comparison with passive attacks is that an active attack can sometimes be detected. But, a stealth attack, which is proposed in recent paper, enables the attacker to do the same kind of active attack with hiding his existence.

Based on this threat analysis and the identified capabilities of the potential attackers, we will now discuss several specific attacks that can target the operation of a routing protocol in an ad hoc network.

- *Location disclosure*: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, or even the structure of the entire network.
- *Black hole*: In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.
- *Replay*: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.
- *Wormhole*: The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, say node A, captures routing traffic at one point of the network and tunnels them to another point in the network, say to node B, that shares a private communication link with A. Node

B then selectively injects tunneled traffic back into the network .The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers.

- *Blackmail*: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated.
- *Denial of service*: Denial of service attacks aim at the complete disruption of the routing function and therefore the whole operation of the ad hoc network. Specific instances of denial of service attacks include the *routing table overflow* and the *sleep deprivation torture*. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.
- *Routing table poisoning*: Routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.
- Impersonation: Current ad hoc routing protocols do not authenticate source IP address. IP address information of a packet can be simply modified by the compromised node or malicious attacker and even MAC address can be changed since most open source device drivers now allow the user to change the MAC address. A malicious node can launch many attacks by altering its MAC or IP address. Both AODV and DSR are susceptible to this attack.

SECURITY REQUIREMENTS OF AD HOC NETWORKS

A good secure routing algorithm prevents each of the exploits presented in Section 4; it must ensure that no node can prevent successful route discovery and maintenance between any other nodes other than by non-participation. In sum, all secure ad hoc routing protocols must satisfy the following requirements to ensure that path discovery from source to destination functions correctly in the presence of malicious adversaries. The term security protocol traditionally refers to authentication protocols, or cryptographic protocols, where the goal is to securely share information (e.g., a message or a session key) between two nodes. Security analysis for authentication protocols evaluates if it is possible for a third party (i.e., the adversary) to obtain

access to the protected key, regardless of intermediate nodes within the communication path [10]. Conversely, security evaluations for MANET secure routing protocols must consider actions taken by intermediate nodes. That is, we must consider whether the intermediate nodes can impact the secure routing protocol's intended goal. More specifically, we must consider route accuracy (securing the route discovery phase) and protocol reliability (securing the data forwarding phase). A routing protocol is considered to maintain route accuracy if it produces routes that exist within the current network topology. Route accuracy is an integrity issue, ensuring that a malicious attacker has not corrupted the path obtained during the route discovery phase. Since the routes obtained during route discovery can fail due to both malicious actions and non malicious failures (e.g., mobility, hardware failures, etc.), the routing protocols must also provide reliability. Once route paths begin to fail, reliability mechanisms identify that the path is no longer operating and initiate a new route discovery process or select an alternate path if multi-path protocols [11] are being utilized. Reliability mechanisms may also attempt to detect and remove malicious nodes via probing protocols.

SECURE AD HOC ROUTING

There exist several proposals that attempt to architect a secure routing protocol for ad hoc networks, in order to offer protection against the attacks mentioned in the previous section. These proposed solutions are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing ones (like DSR and AODV). As we will see, the design of these solutions focuses on providing countermeasures against specific attacks, or sets of attacks. Furthermore, a common design principle in all the examined proposals is the performance-security trade-off balance. Since routing is an essential function of ad hoc networks, the integrated security procedures should not hinder its operation. Another important part of the analysis is the examination of the assumptions and the requirements that each solution depends on. Although a protocol might be able to satisfy certain security constraints, its operational requirements might thwart its successful employment.

ARAN

ARAN was proposed by Sanzgiri et al in 2002 [4] , targeting to combat attacks including unauthorized participation, spoofed route signaling, alteration of routing messages, replay attacks, etc. Similar to other secure routing protocols, ARAN is also a security adds on over on-demand routing protocols. It provides authentication, message integrity and non-repudiation as part of minimal security policy for ad hoc environment.

ARAN stands for Authenticated Routing for Ad hoc Networks. It is motivated to detect and protect against malicious actions by third parties and peers in an ad hoc environment. ARAN is a security scheme, which can be applied to any on-demand routing protocols. It takes the advantages of PKI based digital signature scheme to provide security features including authentication, message integrity and non-repudiation.

ARAN consists of three stages: a preliminary certification process, a mandatory end-to-end authentication stage and an optional stage providing secure shortest path. To deploy these three stages, ARAN requires the use of a trusted certificate server *T* and public key cryptography. Each node, before entering the network, must request a certificate from *T*, and will receive exactly one certificate after securely authenticating their identities to *T*.

We provide a security analysis of ARAN by evaluating its robustness in the presence of the attacks introduced in Section 4. We also compare performance of ARAN to the AODV routing protocol [1].

Unauthorized participation: ARAN participants accept only packets that have been signed with a certified key issued by the trusted authority. In practice, many single-hop 802.11 deployments are already using VPN certificates; this is the case on the UMass campus. Mechanisms for authenticating users to a trusted certificate authority are numerous; a significant list is provided by Schneier. The trusted authority is also a single point of failure and attack, however, multiple redundant authorities may be used (e.g., as by Zhou and Haas [2]). Spoofed Route Signaling: Since only the source node can sign with its own private key, nodes cannot spoof other nodes in route instantiation. Similarly, reply packets include the destination node's certificate and signature, ensuring that only the destination can respond to route discovery. This prevents impersonation attacks where either the source or destination nodes is spoofed.

Fabricated Routing Messages: Messages can be fabricated only by nodes with certificates. In that case, ARAN does not prevent fabrication of routing messages, but it does offer a deterrent by ensuring non-repudiation. A node that continues to inject false messages into the network, may be excluded from future route computation.

Alteration of Routing Messages: ARAN specifies that all fields of RDP and REP packets remain unchanged between source and destination. Since both packet types are signed by the initiating node, any alterations in transit would be immediately detected by intermediary nodes along the path, and the altered packet would be subsequently discarded. Repeated instances of altering packets could cause other nodes to exclude the errant node from routing, though that possibility is not considered here. Thus, modification attacks are prevented.

Securing Shortest Paths: We believe there is no way to guarantee that one path is shorter than another in terms of hop count. Tunneling attacks are possible in ARAN as they are in any secure routing protocol. Securing a shortest path cannot be done by any means except by physical metrics such as a timestamp in routing messages. Accordingly, ARAN does not guarantee a shortest path, but offers a quickest path which is chosen by the RDP that reaches the destination first. Malicious nodes do have the opportunity in ARAN to lengthen the measured time of a path by delaying REPs as they propagate, in the worse case by dropping REPs, as well as delaying routing after path instantiation. Finally, malicious nodes using ARAN could also conspire to elongate all routes but one, forcing the source and destination to pick the unaltered route; clearly, a difficult task.

Replay Attacks: Replay attacks are prevented by including a nonce and a timestamp with routing messages.

SAODV

SAODV proposed by M.G. Zapata, and N. Asokan [9] in 2002. Let's assume that there is a key management sub-system that makes it possible for each ad hoc node to obtain public keys from the other nodes of the network. Further, each ad hoc node is capable of securely verifying the association between the identity of a given ad hoc node and the public key of that node. How this is achieved depends on the key management scheme.

Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). For the non-mutable information, authentication is perform in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information. The information relative to the hash chains and the signatures is transmitted with the AODV message as an extension message that we will refer to as Signature Extension.

SAODV avoids active external attacks by not forwarding route requests to the external nodes. This is done by authenticating all the nodes of the network. In the implementation carried out here the authentication of a node is determined by its password. Here all the nodes of the network are assigned the same password. Hence before forwarding route request to a neighbor, a node first checks the authenticity of the neighboring node by verifying its password. If it is found legal, then only route request is forwarded. In this way, external nodes are excluded from entry into the network. The problem of route table overflow is solved by updating the tables at regular intervals of 70ms. SAODV solves the problem of blackhole by disabling the intermediate nodes to send route replies and thereby allowing the generation of route reply only by the destination node. After receiving route reply from an intermediate node, the originator sends an enquiry to check whether a route from that intermediate node to the destination node exists or not. If it exists, the originator trusts the intermediate node and sends out the data packets via this intermediate node. If not, the originator simply discards the reply message from the intermediate node, sends out alarm message to the network, isolates that intermediate node from the network and starts a new route discovery process. No malicious node can read the data in the data packet due to the encryption of the message. Every node checks password before forwarding the RREQ. All nodes on the route from source to destination are secure and fulfill security requirements of the sender.

SAR

There is another approach to secure the ad hoc routing protocol motivated from traditional wired routing matrices where same security levels of nodes incorporate each other [13]. Instead of discovering the shortest path between two nodes, Security Aware Ad Hoc Routing (SAR) protocol can discover a path with desired security attributes, such as a path through nodes a particular shared key. For this purpose to determining a secure route, the information in the routing messages must be protected against alteration that can change routing behavior. A node initiating route discovery determines the required minimal trust level for nodes participating in the query and reply propagation. Since only nodes at each trust level share symmetric encryption keys, intermediate nodes of different levels cannot decrypt in-transit routing packets or determine whether the

required security attributes can be satisfied and drop them. Only the nodes with the correct key can read the header and forward the packet. So if a packet has reached the destination, it must have been propagated by nodes at the same level. Therefore Routes discovered by SAR come with "quality of protection" guarantees.

One of the merits SAR has is that it can be implemented based on any on-demand ad hoc routing protocol with suitable modification [13]. The security metric can be embedded into RREQ packet. It also showed the practical implementation and experimental data by mixing with AODV [14]. Drawback of SAR Although SAR scheme provides protection of the routing protocol traffic; it does not eliminate false routing information provided by malicious nodes. Moreover, the assumed supervising organization and the fixed assignment of trust levels do not pertain to the ad hoc paradigm. And SAR has also a lot of encryption overhead, since each intermediate node has to perform it.

SRP

SRP focus on bi-directional communication between a pair of nodes. A *security association (SA)* between the *source node S* and the *destination node T* is assumed. The trust relationship could be instantiated, for example, by the knowledge of the public key of the other communicating end. The two nodes can negotiate a shared secret key, e.g., via the Elliptic Curve Diffie-Hellman algorithm [12], and then, using the *SA*, verify that the principal that participated in the exchange was indeed the trusted node. For the rest of the discussion, we assume the existence of a shared key *KS,T*. The *SA* is bi-directional in that the shared key can be used for control (data) traffic flow in both directions. Relevant state has to be maintained for each direction though.

SRP makes efficient use of the security association between the two communicating nodes *S* and *T*. Route request packets verifiably propagate to the destination (in the general case) and route replies are returned to *S* strictly over the reversed route, as accumulated in the route request packet. Similarly, route error messages can only be generated by nodes that lie on the route that is reported as broken. In order to guarantee this functionality of crucial importance, *SRP* determines explicitly the interaction with the network layer; i.e., the *IP*-related functionality. Furthermore, it provides a novel way of query identification, which protects the query propagation and the end-nodes from *DoS* attacks. Finally, propagating query packets are handled locally by a *priority scheme* that enhances the robustness and the responsiveness of the protocol.

This figure shows SRP as an extension of a reactive routing protocol: the SRP header is appended to the basis routing protocol header.

SRP consists of several security extensions that can be applied to existing ad hoc routing protocols providing end-to-end authentication. The operational requirement of SRP is the existence of a security association between every source and destination node. The security association is used to establish a shared secret between the two nodes, and the non-mutable fields of the exchanged routing messages are protected by this shared secret.

IP Header
Basis Routing Protocol Packet
SRP Header

Protocols	**Attacks**					
	Location disclosure	**Black hole**	**Replay**	**Wormhole**	**Denial-of-service**	**Routing table poisoning**
ARAN	NO	NO	YES	NO	NO	YES
SAODV	NO	NO	YES	NO	NO	YES
SAR	NO	NO	YES	NO	NO	YES
SRP	NO	NO	YES	NO	YES	YES

Defense against attacks.

CONCLUSION

Secure Routing is one of the most basic and important tasks in a collaborative computer network. This review presented the security flaws of AODV and routing protocols which provide security over the AODV. However, a difficult problem is how to guarantee these desirable properties. Neither simulations nor testbed implementations can ensure the quality required for these protocols. As an alternative to these methods, some researchers have successfully investigated the use of formal verification as a mean to guarantee the quality of routing protocols. Formal verification is a technique that assures a system has, or has not, a given property, based on a formal specification of the system under evaluation.

We conclude that more work is needed towards a formal model based on solid mathematical grounds that can precisely give a definition for secure ad hoc routing. This will allow researchers to formally prove whether a proposed protocol satisfies the definition under certain assumptions and will make the comparison between the properties of each proposal an easier and well-structured process.

REFERENCES

1. Das S. Perkins C.E., Belding-Royer E.M. Ad-hoc on-demand distance vector (aodv) routing. RFC 3561, IETF Network Working Group, 2003.

2. L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network Magazine, 13(6):24–30, November/December 1999.

3. S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pages 255–265, 2000.

4. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", *Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02)*, IEEE Press, 2002, pp. 78-87.

5. J.-P. HuBaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In Proc. ACM MOBICOM, Oct. 2001.

6. J. Kong et al. Providing robust and ubiquitous security support for mobile ad-hoc networks. In Proc. IEEE ICNP, pages 251–260, 2001.

7. S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. In Proc. ACM Mobihoc, 2001.

8. P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

9. M.G. Zapata, and N. Asokan, "Secure Ad hoc On-Demand Distance Vector Routing," *ACM Mobile Computing and Communications Review*, vol. 3, no. 6, July 2002, pp. 106-10

10. Mitchell, J. C., Mitchell, M., Stern, U. : Automated Analysis of Cryptographic Protocols Using Murphi. IEEE Symposium on Security and Privacy. (1997) 141–151

11. Dolev, D., Yao, A.C.: On the security of public key protocols. IEEE Transactions on Information Theory. 29(12) (1983) 198–208

12. W. Diffie, M.E. Hellman, "New directions in cryptography," IEEE Transactions in Information Theory, 1976.

13. Zheng Yan, "Security in Ad Hoc Networks", Networking Laboratory, Helsinki University of Technology, 2001

14. S. Yi, P. Naldurg, and R. Kravets. Security-aware ad-hoc routing for wireless networks. Technical Report UIUCDCS-R-2001-2241, University of Illinois at Urbana-Champaign, August 2001.