International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)

International Conference on Information Systems and Computing (ICISC-2013), INDIA.

PDIR:PRE-DEPLOYED INFRASTRUCTURE ROUTING FOR SECURE AD HOC NETWORKS

Sridevi.N[1], Amirthasaravanan.A[2], Divya.S[3]

[1,2,3]*Department of Information Technology, University College of Engineering Villupuram, Villupuram,India.*

E-mail: sridevi.792@gmail.com, aasaravanan777@gmail.com , champdivyas@gmail.com

Abstract

Secured routing is the emerging issue in ad hoc networks. One of the major problems in routing is malicious attacks, which are not only possible from outsider nodes but also from compromised nodes within the network. This vulnerability will affect the integrity of the network. In this paper we have created a trusted third party certification authority, which will allow only certified nodes to connect with the network and it will also avoid misbehaviors in routing. In our proposed system we will create an authenticated and secured routing for the ad hoc network in two stages. In the stage (1), our goal is to verify that the intended destination was reached .In stage (2), data transfer can be pipelined with its shortest path discovery operation. So we can prevent nodes from changing their paths. We are using cryptographic certificates for the purpose of authentication and non-repudiation. So malicious nodes cannot alter the path length and hence integrity of the encrypted data can maintain.

***Keywords*-- Trusted Third Party Certification, Cryptographic Certificates, Authentication**

I. INTRODUCTION

Ad hoc networks are autonomous networks operating either in isolation or as "stub networks" connecting to a fixed network. Mobile ad hoc networks (MANETs) are infrastructure less and intercommunicate using single-hop and multi-hop paths. [19] Do not necessarily rely on existing infrastructure. No "access point". Each node serves as a router and forwards packets for other nodes in the network. Topology of the network continuously changes

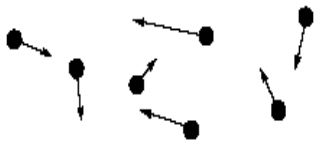

Fig1.An Ad hoc network with nodes moving in different directions and speeds.

Ad hoc network use mobile nodes to enable communication outside transmission range. In a multi hop wireless Ad hoc network[15], mobile nodes cooperate to form a network without using any infrastructure such as access points or base stations. Instead, the mobile nodes forward packets for each other, allowing communication among nodes outside wireless transmission range. The nodes mobility and fundamentally limited capacity of the wireless medium, together with wireless transmission effect such as attenuation, multipath propagation, and interference, combine to create significant challenges for routing protocols operating in an Ad hoc network [6].

Attacks on Ad hoc network routing protocols disrupt network performance and reliability. In this paper we discuss to avoid it.

All or some nodes within an ad hoc are expected to be able to route data-packets for other nodes in the network who want to reach other nodes beyond their own transmission range. This is called peer-level multi-hopping and is the base for ad hoc networks that constructs the interconnecting structure for the mobile nodes. An ad hoc network is usually thought of as a network with nodes that are relatively mobile compared to a wired network. Hence the topology of the network is much more dynamic and the changes often unpredictable oppose to the Internet which is a wired network. This fact creates many challenging research issues since the objectives of how routing should take place is often unclear because of the different resources like bandwidth, battery power and demands like latency and other types of QoS.

II. CHARACTERISTICS OF ADHOC NETWORKS

1. Dynamic topology
2. Heterogeneity
3. Bandwidth-constrained variable capacity links
4. Limited physical security
5. Nodes with limited battery life and storage capabilities

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

III. SECURITY GOALS

3.1 Availability

Ensures survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g., key management service.

3.2 Confidentiality

Ensures certain information is never disclosed to unauthorized entities.

3.3 Integrity

Message being transmitted is never corrupted.

3.4 Authentication

Enables a node for ensuring the identity of the peer node, which is communicating.

Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

3.5 Non-repudiation

Ensures that the origin of a message cannot deny having sent the message.

IV. CHALLENGE

Use of wireless links renders an Ad-hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Eavesdropping might give an attacker access to secret information thus violating confidentiality. [18] We need to consider malicious attacks not only from outside but also from within the network from compromised nodes. For high survivability Ad-hoc networks should have a distributed architecture with no central entities, centrality increases vulnerability. Ad-hoc network is dynamic due to frequent changes in topology. Security mechanism need to be on the fly (dynamic) and not static and should be scalable.

4.1 Problems with Existing Ad-Hoc Routing Protocols

4.1.1 Implicit trust relationship between neighbors

Current Ad-hoc routing protocols[16] [17] inherently trust all participants. Most Ad-hoc routing protocols are cooperative by nature and depend on neighboring nodes to route packets.

This naïve trust model allows malicious nodes to paralyze an Ad-hoc network by inserting erroneous routing updates, replaying old messages, changing routing updates or advertising incorrect routing information. While these attacks are possible in fixed network as well, the Ad-hoc environment magnifies this makes detection difficult.

a) S->A->B->C->D->X-->M

b) S->A->B->M->C->-D->X

Fig2. a) and b) Trusted Relationship Between Neighbors

4.1.2 Throughput

Ad-hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave by agreeing to forward the packets and failing to do so, because it is overloaded, selfish, and malicious or broken. Misbehaving nodes can be a significant problem. Although the average loss in throughput due to misbehaving nodes is not too high, in the worst case it is very high

4.1.3 Attacks using modifications of protocol fields of messages

Current routing protocols assume that nodes do not alter the protocol field of messages passed among nodes. Since the level of trust in a traditional Ad-hoc network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets [15] to disrupt communication.

Malicious nodes can easily cause redirection of network traffic and DOS attacks by simply altering these fields. For example, in the network illustrated in Figure A & B a malicious node M could keep traffic from reaching X by consistently advertising to B a shorter route to X than the route to X, which C is advertising.

V. ATTACKS ON AD-HOC NETWORK

5.1 Routing-disruption attacks

The attacker attempts to cause legitimate data packets to be routed in dysfunctional ways.

5.2 Resource-consumption attacks

The attacker injects packets into the network in an attempt to consume valuable network resource such as bandwidth or to consume node resource such as memory (storage) or computation power.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

VI. SOLUTIONS TO PROBLEMS IN AD-HOC ROUTING

6.1 Using pre-deployed security infrastructure

Here we assume existence of certain amount of security infrastructure. The type of Ad-hoc environment that we are dealing with here is called managed-open environment.

6.1.1 Assumptions

A managed-open environment assumes that there is opportunity for pre-deployment .Nodes wishing to communicate can exchange initialization parameters before hand, perhaps within the security of an infrastructure network where session keys[1] may be exchanged or through a trusted third party like a certification authority.

6.2 ARAN protocol in managed-open environment:

ARAN or Authenticated Routing for Ad-hoc Networks detects and protects against malicious actions by third parties and peers in Ad-hoc environment. ARAN introduces authentication, message integrity and non-repudiation to an Ad-hoc environment. ARAN is composed of two distinct stages. The first stage is simple and requires little extra work from peers beyond traditional ad hoc protocols. Nodes that perform the optional second stage increase the security of their route, but incur additional cost for their ad hoc peers who may not comply(e.g., if they are low on battery resources).ARAN makes use of cryptographic certificates for the purpose of authentication and non-repudiation.

6.2.1 Stage 1

It contains a preliminary certification stage and a mandatory end-end authentication stage. It is a lightweight stage and does not demand too many resources.

6.2.1.1 Preliminary Certification

ARAN requires the use of a trusted certificate server T. Before entering the Ad-hoc network, each node requests a certificate from T. For a node A,

T->A : Cert(A)=[IP(A),K(A)+,t,e]K(T)

The certificate contains the IP address of A, the public key [1] of A, a timestamp t of when the certificate was created and a time e at which the certificate expires. These variables are concatenated and signed by T. All nodes must maintain fresh certificates with the trusted server and must know T's public key.

6.2.1.2 End-to-End authentication

The goal of stage 1 is for the source trusts the destination to choose the return path.

6.2.1.2.1 Source node

A source node, A, begins route instantiation to a destination X by broadcasting to its neighbors a route discovery packet (RDP).

A->broadcast [RDP,IP(X),CERT(A),N(A),t] K(A)

The RDP includes a packet type identifier("RDP"),the IP address of the destination[IP(X)],A's certificate [Cert(A)],a nonce N(A),and the current time t, all signed with A's private key. Each time A performs route discovery, it monotonically increases the nonce. Nodes then store the nonce they have last seen with its timestamp.

6.2.1.2.2 Intermediate node for RDP

Each node records the neighbor from which it received the message. It then forwards the message to each of its neighbors, signing the contents of the message. This signature prevents spoofing attacks that may alter the route or form loops. Let A's neighbor be B,

B->broadcast
[[RDP,IP(X),CERT(A),N(A),t]K(A)-]K(B)-,CERT(B)

Nodes do not forward messages for which they have already seen the [N(A),IP(A)] tuple. Upon receiving the broadcast, B's neighbor C validates the signature with the given certificate. C then rebroadcasts the RDP to its neighbors, first removing B's signature.

C-> broadcast:
[RDP,IP(X),CERT(A),N(A),t] K(A)-]K(C)-,CERT(C)

6.2.1.2.3 Destination node

Eventually, the message is received by the destination, X, who replies to the first RDP [15] that it receives for a source and a given nonce. There is no guarantee that the first RDP received traveled along the shortest path from the source. The destination unicasts a Reply (REP) packet back along the reverse path to the source.

X->D:broadcast
[REP,IP(A),Cert(X),N(A),t]K(X)-

6.2.1.2.4 Intermediate node for REP

Nodes that receive the REP forward the packet back to the predecessor from which they received the original RDP. All REP's are signed by the sender. Let D's next hop to the source is node C.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

D->C
[REP,IP(A),Cert(X),N(A),t]K(X)-] K(D)-,Cert(D)

C validates D's signature, removes the signature, and then signs the contents of the message before unicasting the RDP to B

C->B:
[REP,IP(A),Cert(X),N(A),t]K(X)-] K(C)-,Cert(C)

A node checks the signature of the previous hop as the REP is returned to the source. This avoids attacks where malicious nodes instantiate routes by impersonation and re-play of X's message.

6.2.1.2.5 Source node

When the source receives the REP, it verifies that the correct nonce was returned by the destination as well as the destination's signature[9] [6]. Only the destination can answer an RDP packet. Other nodes that already have paths to the destination cannot reply for the destination. While other protocols allow this networking optimization, we note that removing it also removes several possible exploits and cuts down on the reply traffic received by the source. Because only the destination can send REP's, loop freedom is guaranteed easily.

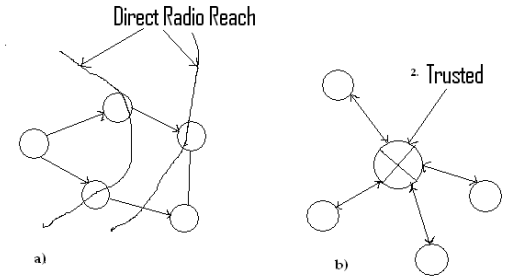

Fig.3. a) Routing in Ad hoc network b) secured Routing in Ad hoc

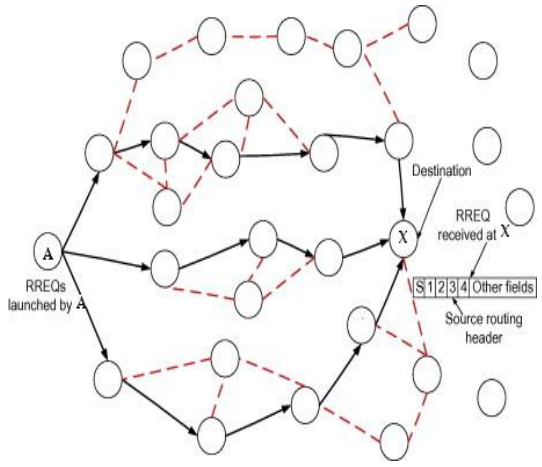

Fig4.Route Discovery in Ad Hoc Network

6.2.2 Stage 2

Stage (2) is done only after stage (1) is over. This is because the destination certificate is required in Stage (2).This stage is primarily used for discovery of shortest path in a secure fashion. Since a path is already discovered in Stage (2),data transfer can be pipelined with Stage (2)'s shortest path discovery operation.

6.2.2.1 Source node

The source begins by broadcasting a Shortest Path Confirmation (SPC) message to its neighbors (the same variables are used as in stage 1).

A->broadcast:
[SPC,IP(X),Cert(X)[[IP(X),Cert(X),
N(A),t] K(A)-]K(X)-

The SPC message begins with the SPC packet identifier ("SPC"),X's IP address and certificate. The source concatenates a signed message containing the IP address of X, its certificate, a nonce and timestamp. This signed message is encrypted with X's public key so that other nodes cannot modify the contents.

6.2.2.2 Intermediate Node

A neighbor B that receives the message rebroadcasts the message after including its own cryptographic credentials signs the encrypted portion of the received SPC, includes its own certificate, and re-encrypts with the public key of X. This public key can be obtained in the certificate forwarded by A.

B->broadcast
[SPC,IP(X),Cert(X)[[[IP(X),Cert(X), N(A),t] K(A)-
]K(X)+,Cert(B)]K(X)+

Nodes that receive the SPC packet create entries in their routing table so as not to forward duplicate packets. The entry also serves to route the reply packet from the destination along the reverse path.

6.2.2.3 Destination Node

Once the destination X receives the SPC ,it checks that all the signatures are valid. X replies
to the first SPC it receives and also any SPC with a shorter recorded path. X sendsa Recorded Shortest Path(RSP) message to the source through its predecessor D.

X->D[RSP,IP(A),Cert(X),N(A),ROUTE]
K(X)-

The source eventually receives the packet and verifies that the nonce corresponds to the SPC is originally generated.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

6.4 Advantages

The onion-like signing of messages prevents nodes in the middle from changing the path in several ways. First, to increase the path length of the SPC, malicious nodes require an additional valid certificate. Second, malicious nodes cannot decrease the recorded path length or alter it because doing so would break the integrity of the encrypted data.

VII. Route Maintanence

Nodes keep track of whether routes are active. When no traffic has occurred on an existing route for that route's lifetime, the route us simply de-activated in the route table. Data received on an inactive route causes nodes to generate an Error (ERR) message that travels the reverse path towards the source. Nodes also use ERR messages to report links in active routes that are broken due to node movement. All ERR message must be signed. For a route between source A and destination X, a node B generates the ERR message for its neighbor C as follows,

B->C
[ERR,IP(A),IP(X),Cert(C),N(B),t]
K(B)-

This message is forwarded along the path towards the source without modification. A nonce and timestamp ensures the ERR message is fresh. Because messages are signed, malicious nodes cannot generate ERR messages for other nodes. The non-repudiation provided by the signed ERR message allows a node to be verified as the source of each ERR message that it sends. A node which transmits a large number of ERR messages, whether the ERR messages are valid or fabricated, should be avoided.

VIII. Key Revocation

ARAN attempts a best effort key revocation that is backed up with limited time certificates. In the event that a certificate needs to be revoked, the trusted certificate server, T, sends a broadcast message to the ad hoc group that announces the revocation. Calling the revoked certificate cert r, the transmission appears as:

T->broadcast
[revoke, Cert(R)]K(T)-

Any node receiving this message re-broadcasts it to its neighbors. Revocation notices need to be stored until the revoked certificate would have expired normally. Any neighbor of the node with the revoked certificate needs to reform routing as necessary to avoid transmission through the now-untrusted node.

This method is not failsafe. If an untrusted node, whose certificate is being revoked, is the only link between 2 parts of an Ad-hoc network, It may not propagate the revocation message to the other part-leading to a partitioned network.

To detect this situation and to hasten the propagation of revocation notices, when a node meets a new neighbor, it can exchange a summary of its revocation notices with that neighbor. If these summaries do not match, the actual signed can be forwarded and re-broadcasts to restart propagation of the notice.

IX. Secure-Aware Routing

It makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decision. Current routing protocols discover the shortest path between two nodes. But we can discover a path with security attributes (e.g., a path through nods with a particular shared key). A node initiating route discovery sets the sought security level for the route i.e., the required minimal trust level for nodes participating in the query/reply propagation. Node at each trust level share symmetric encryption keys[1] [6].

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, since only they can decrypt the packet, see its header and forward it.

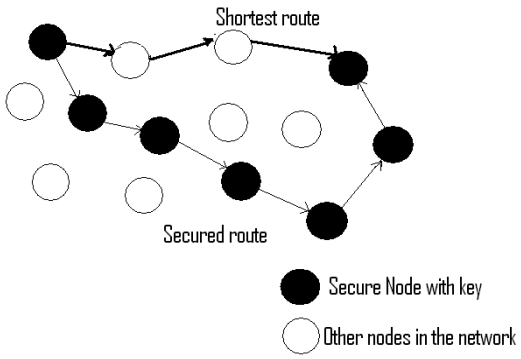

Fig.4. Secured route

9.1 Implementation

The RREQ (Route REQuest) and the RREP (Route REPly) packets formats are modified to carry additional security information.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

The RREQ packet has an additional field called RQ_SEC_REQUIREMENT that indicates the required security level for the sender wishes to discover.

This could be a bit vector. An intermediate node at the required trust level, updates the RREQ packet by updating another new field ,RQ_SEC_GUARANTEE field. The RQ_S8EC_GUARANTEE [15] field contains the minimum security offered in the route. This can be achieved if each intermediate node at the required trust level performs an 'AND' operation with RQ_SEC_GUARANTEE field it receives and puts the updated value back into the RQ_SEC_GUARANTEE field forwarding the packet.

Finally, the packet reaches the destination if a route exists. In the RREP packet one additional field is also added. When an RREQ successfully traverses the network to the sender, the RQ_SEC_GUARANTEE represents the minimum security level in the entire path from source to destination. So the destination copies this from the RREQ to the RREP, into a new field called RP_SEC_GUARANTEE field.

The sender can use this value to determine the security level on the whole path, since the sender can find routes which offer more security than asked for, with which he can make informed decisions.

X. CONCLUSIONS

We have presented the solution for the problems in existing security scenario in the Ad-hoc network environment. Key management and Ad-hoc routing aspects of wireless Ad-hoc networks were discussed. Ad-hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. The authenticated protocols are still very expensive and not fail safe. Several protocols for routing in Ad-hoc networks have been proposed. There is a need to make them secure and robust to adapt to the demanding requirements of these networks. Intrusion detection is a critical security area .But the flexibility, ease and speed with which these networks can be set up implies they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application.

REFERENCES

[1] J. Cha, J. Cheon, An identity-based signature from gap Diffie–Hellman groups, in: Proc. International Workshop on Practice and Theory in Public Key Cryptography, LNCS, Springer, 2003, pp. 18–30.

[2] H.-Y. Chien, R.-Y. Lin, Identity-based key agreement protocol for mobile ad-hoc networks using bilinear pairing, in: Proc. Sensor Networks, Ubiquitous, and Trustworthy Computing, IEEE, 2006, pp. 1145 520–529.

[3] H.-Y. Chien, R.-Y. Lin, Improved id-based security framework for ad 1147 hoc network, Ad Hoc Netw. 6 (1) (2008) pp.47–60.

[4] T. Clausen, P. Jacquet, RFC3626 –Optimized Link State Routing Protocol (OLSR), 2003.

[5] H. Deng, D.P. Agrawal, TIDS: threshold and identity-based security scheme for wireless ad hoc networks, Ad Hoc Netw. 2 (3) (2004) pp.291–307.

[6] H. Deng, A. Mukherjee, D.P. Agrawal, Threshold and identity-based key management and authentication for wireless ad hoc networks, in: Proc. ITCC, IEEE, 2004, pp. 107–111.

[7] S. Goldwasser, S. Micali, R.L. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, J. SIAM Comput. 17 1158(April) (1988) 281–308.

[8] F. Hess, Efficient identity based signature schemes based on pairings, in: Proc. SAC: Annual International Workshop on Selected Areas in Cryptography, LNCS, Springer, 2003, pp. 310–324.

[9] A. Khalili, J. Katz, W.A. Arbaugh, Toward secure key distribution in truly ad-hoc networks, in: Proc. SAINT Workshops, IEEE, 2003, pp. 342–346.

[10] F. Kuhn, R. Wattenhofer, A. Zollinger, Asymptotically optimal geometric mobile ad-hoc routing, in: 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, DIALM'02, 2002.

[11] W. Lee, W. Sriborrirux, Optimizing authentication mechanisms using ID-based cryptography in ad hoc wireless mobile networks, in: Proc. Information Networking, Networking Technologies for Broadband and Mobile Networks, LNCS, Springer, 2004, pp. 925–934.

[12] Y.-H. Lee, H. Kim, B. Chung, J. Lee, H. Yoon, On-demand secure routing protocol for ad hoc network using id based cryptosystem, in: Proc. 4th ICPDCAT, IEEE, 2003, pp. 211–215.

[13] G. Li, W. Han, A new scheme for key management in ad hoc networks, in: Proc. 4th International Conference on Networking Proceedings, LNCS, Springer, 2005, pp. 242–249.

[14] J.V.D. Merwe, D. Dawoud, S. McDonald, A survey on peer-to-peer key management for mobile ad hoc networks, ACM Comput. Surv. 39 (1) (2007) pp.1–45.

[15] B.-N. Park, W. Lee, ISMANET: a secure routing protocol using identity-based encryption scheme for mobile ad-hoc networks, J. IEICE Trans. Commun. (2005) pp.2548–2556.

[16] B.-N. Park, J. Myung, W. Lee, ISSRP: a secure routing protocol using identity-based sign encryption scheme in ad-hoc networks, in: Proc. 5th International Conference on Parallel and Distributed Computing, LNCS, Springer, 2004, pp. 711–714.

[17] B.-N. Park, J. Myung, W. Lee, LSRP: a lightweight secure routing protocol with low cost for ad-hoc networks, in: Proc. International Conference on Convergence in Broadband and Mobile Networking, LNCS, Springer, 2005, pp. 160–169.

[18] K.G. Paterson, ID-Based Signatures from Pairings on Elliptic Curves. Report 2002/004, Cryptology ePrint Archive, 2002.

[19] C.K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, 2001.

[20] L. Zhou, Z. Haas, Securing ad hoc networks, IEEE Network Magazine 13 (6) (Nov/Dec 1999) pp.24–30.