Authentication Schemes for Open Distributed Network: A Classification

Deepak Kumar
Research Scholar
Department of Computer Science
Faculty of Technology
Gurukul Kangri
Vishwavidyalaya, Haridwar,
Uttarakhand, India.

Vinod Kumar
Professor and Head
Department of Computer Science.
Faculty of Technology
Gurukul Kangri
Vishwavidyalaya,Haridwar,
Uttarakhand, India

ABSTRACT
An authentication protocol is a sequence of message exchanges between entities that either distributes secrets to some of those principals or allows the use of some secret to be recognized .Distributed Network, such as sensor and mobile ad hoc networks, must conquer a numerous of security challenges to realize their potential in both civil and military applications. Usually, a Distributed Network like ad hoc networks are deployed in untrusted environments. Therefore, authentication is a pioneer to any secure interactions in these networks. Recently, various authentication protocols have been proposed for ad hoc networks. In distributed authentication services in ad hoc networks. Two nodes authenticate each other via signed, unforgeable certificates released by a ”virtual“ trusted certification authority. Compared with regular network authentication solutions [28, 29] that rely on physically present, third-party trusted (certification authority) server(s), our design takes a self organized securing approach, in which multiple nodes (say, k) collaboratively serve the role of a certification authority server. Therefore, the authority and functionality of the authentication server are spread to each node's locality. Any local k nodes are trusted as a whole and collaboratively provide authentication services. This paper describes the authentication procedure and a classification that clarifies similarities and differences among authentication protocol described in the literature. The classification is based upon the role of nodes in the authentication function, establishment of certificate, and type of certificate.

General Terms
Authentication, Protocol Classification, Ad Hoc Networks, Distributed System, Identity Verification..

Keywords
Routing, Authentication, Certification, Security, Validation.

1. INTRODUCTION
A distributed system—a collection of hosts interconnected by a network—poses some complex security problems. In a distributed system, the hosts communicate by transferring and receiving messages over the network. Various resources (like files and printers) distributed among the hosts are shared across the network in the form of network services provided by servers. Individual processes (clients) that desire access to resources direct service requests to the appropriate servers. The another category of such system is Ad-hoc networks. Ad-hoc networks are a new standard of wireless communication for mobile hosts. No set infrastructure such as base stations as mobile switching Node mobility causes frequent changes in topology. Nodes within the radio range communicate directly via wireless links while those which are remote to one side rely on other nodes to broadcast messages. The attack could be launched at any layer of an ad hoc network. Confidentiality ensures that confidential information is never unfolded to unauthorized entities. Integrity sure that a message being transferred is never tainted. Authentication empowers a node to ensure the identity of the look up node it is communicating with. Finally, non-repudiation message. We ponder that authentication is the building block service, since other services depend on the authentication of communication entities[19] [7].Authentication supports privacy ensures that the origin of a message cannot neglect having sent the protection by ensuring that entities verify and validate one another before disclosing any secret information. In addition, it supports confidentiality and access control, by allowing access to services and infrastructure to authorized entities only, while denying unauthorized entities access to sensitive data. A significant number of authentication protocols have recently been proposed for ad hoc networks; examples include [1] [2] [3] [4] [5] [6] [8] [9] [10] [11] [12] [13] [17] [18] [19] [24]. A classification is needed to understand the similarities between sets of related protocols and to realize the motivation behind each. A classification also enables us to better scrutinize and compare protocols with respect to their category rather than comparing individual protocols; to recognize common drawbacks and attacks against each class of authentication protocols; and to identify common tectonic elements in each class. This paper presents a classification of authentication protocols in distributed networks. The paper also prompts the need for authentication management architecture and presents some open research issues. The rest of this paper is organized as follows. In section 2 we introduce the different mechanism of the authentication procedure in an ad hoc network and the authentication status of a supplicant (the entity requesting authentication). In section 3 we provide an overview of our classification and present the three classification criteria proposed. In sections 4, 5 and 6 we discuss each of the three primary classes of the classification. Finally, section 7 concludes the paper and discusses directions for future work.

2. AUTHENTICATION INDISTRIBUTED NETWORKS
Authentication intended to identification plus verification. Identification is the procedure wherefrom an individual claim a certain identity, that claim is checked by verification procedure .Authentication protocols may be retained TTP as part of the authentication protocol Thus the correctness of an authentication

depend on the verification procedure employed. The entities in a distributed system that can be clearly identified are collectively marked to as principals. There are three main types of authentication of interest in a distributed system:

(1) Message content authentication confirms that the content of a message received is the same as when it was sent. (2) message origin authentication verifying the sender (3) General identity authentication calibrate that the principal's identity is as claimed.

(1) Is generally handled by attaching a key-dependent message authentication code (MAC) with a message before it is sent. Message integrity can be confirmed at the receiving side by recomputing the MAC and comparing it with the one attached. (2) Is a subclass of (3) A successful general identity authentication results in a credence held by the authenticating entity (the verifier) that the authenticated entity(the claimant) possesses the claimed identity. Hence succeeding claimant actions are attributable to the claimed identity. General identity authentication is desirable for both authorization and accounting functions. In a distributed environment, authentication has come into existence using a protocol involving message exchanges. We mention to these protocols as authentication protocols. We restrict our attention to general identity authentication only for classification. In an environment where both host and communication compromises can occur, principals must accept a mutually dubious attitude toward one another. Consequently, mutual authentication, whereby both communicating principals rather than performing one-way authentication, they verify each other's identity, whereby only one principal verifies the identity of the other principal, is typically required.

2.1 Mechanism of the Authentication Procedure

Authentication function consists of Following Steps, Certification of Authorized Nodes, Authenticated Route Finding, Authenticated Route Arrangement, Route Repairs, Key Revocation. The routing messages are authenticated end-to-end .Only authorized nodes participate at each hop between source and destination. The pre-authentication procedure is where a requester presents its certificate to an authenticator in an attempt to confirm its eligibility to access determinate resources or offer services. In [5] new nodes must disclose information of the global network key (using challenge response ,for example).After the requester's certificate verification, a certificate installation procedure is invoked to install the requester's new certificate, which it will use as a proof of its identity and as a verification of its certified state thereafter. A certificate could be a symmetric key, a public/private key pair, a convincement of a hash key chain, or some appropriate information. The recognized certificates might be labeled with time stamp an running out after which the requester has to re-negotiate a new "certificate" of certificates. In [5], a node is allocated a portion of the network's private key in a (k, n) gateway of cryptography mechanism. In [2], the authenticating sides use a chain of trust founded between nodes in their trusted list to produce and perform a key exchange between them. In [13], a guarantee key to a TESLA [22] based one-way key-chain is generated and distributed as a node's certificate .After Successful completion of all of the steps above, a requester is pondered authenticated, which means that it is authorized to access resources protected by the authenticator. All communication between the requester and the authenticator is validated at the destination using the established certificate and authenticated by the source. While authenticated, a requester's performance is monitored for fear of its being compromised or misbehaving. A compromise requester may get its certificate cancelled (as in [31]) or its re-establishment of the certificate request denied when its certificates expire. In both cases, the requester is isolated from the network. While authenticated, a requester's behavior is monitored for fear of its being compromised or misbehaving. A compromise requester may get its certificate cancelled (as in [31]) or its re-establishment of the certificate request denied when its certificates expire. In both cases, the requester is isolated from the network.

Public key of node A.	P_{A+}
Private key of node A.	P_{A-}
Symmetric key shared by nodes A and B.	P_{AB}
Encryption of data d with key PA+ .	$\{d\}P_{A+}$
Data d digitally signed by node A. certA Certificate belonging to node A.	$[d]P_{A-}$
Certificate expiration time.	e
Nonce issued by node A. IPA IP address of node A.	N_A
Route Discovery Packet identifier.	RDP
Reply packet identifier.	REP
timestamp.	t

Table-1

2.2 Certification of Authorized Nodes

Authentication Procedure uses cryptographic certificates to bring authentication, message-integrity and non-confutation to the route discovery process. Therefore an authentication procedure requires the use of a trusted certificate server T, whose public key is known to all valid nodes (or multiple servers may be used [30]). Nodes use these certificates during the exchange of routing messages to authenticate themselves to other nodes. The public keys and certificates is commonly used in many secure ad hoc routing protocols, but most suppose the being of such information without any explicit description of how it is transmitted. A node A receives a certificate from T as follows:

$$T \rightarrow A: certA = [IPA, PA+, t, e]PT -$$

The certificate contains the IP address of A (IPA), the public key of A (PA+), a timestamp t of when the certificate was created, and a time e at which the certificate expires. Table-1 summarizes our notation.

2.3 Authenticated Route Finding

The objective of end-to-end authentication is for the source to verify that the proposed destination was reached. The source trusted on the return path that is send back by destination. The source node, A, begins route instantiation to destination X by broadcasting to its neighbors a route discovery packet (RDP):

A → broadcast: [RDP, IPX , NA]PA−, certA

The RDP includes a packet type identifier ("RDP"), the IP address of the destination (IPX), A's certificate (certA) and a nonce NA , all signed with A's private key.

When a node receives an RDP message, it installs a reverse path back to the source by storing the neighbor from which it received the RDP. Let B be a neighbor that has received from A the RDP broadcast, which it subsequently rebroadcasts.

B → broadcast : [[RDP, IPX , NA]PA−]PB− , certA , certB

After receiving the RDP, B's neighbor C validates the signatures for both B andA, the RDP initiator.C then rebroadcasts the RDP.

C → broadcast : [[RDP, IPX , NA] PA −]PC − , certA , certC Each midway node along the path repeats the same steps as C .

2.4 Authenticated Route Arrangement

The destination receiving the RDP, after that it unicasts a Reply (REP) packet back along the reverse path to the source. Let the first node that receives the REP sent by X to be node D. X → D: [REP, IPA, NA]PX − , certx . The REP contains the IP address of A (IPA) as a packet type identifier ("REP"), the certificate associated with X (certx) and the nonce sent by A. Each node which receives the REP forward the packet back to its predecessor from which it received the original RDP. Each node signs the REP and appends its own certificate before forwarding the REP to the next hop, along the reverse path back to the source. Let D's next hop to the source be node C .

D → C: [[REP, IPA , NA]PA −]PD− , certX , certD

C validate D's signature on the REP, take away the signature and certificate, then signs the stuffing of the message and appends its individual certificate before unicasting the REP to B.

C → B: [[REP, IPA, NA]PX −]PC − , certx , certC Each node make sure the nonce and signature of the preceding hop as the REP is returned to the source. This stay away from attacks where malicious nodes instantiate routes by masquerade and replay of X's message. The source receives the REP, it verifies the destination's signature and the nonce returned by the destination.

2.5 Route Repairs

The entry of a route's lifetime is simply deactivated for the existing route where no traffic has occurred. The nodes generate an error (ERR) message whenever nodes received data on an inactive route. This ERR messages also use to report links in active routes that are broken due to node movement. All ERR messages have to be validate. For a route between source A and destination X, a node C generates the ERR message for its neighbor B as follows:

C → B : [ERR, IPA , IPX , Nc]PC − , certc This message is forwarded along the path toward the source without alteration. A nonce make sure that the ERR message is fresh. It is really difficult to identify when ERR messages are fictitious for links that are really active and not broken. However, the signature on the message prevents impersonation and enables non-repudiation. A node should be avoided that transmits a large number of ERR messages, whether the ERR messages are valid or fanciful.

2.6 Key Revocation

The required certificate revocation mechanism must be very reliable and expensive in several environments with strict security criteria. The best-effort immediate revocation service can be provided that is backed up by the use of limited-time certificates due to the desired low overhead in wireless networks and the lower standards of security. The trusted certificate server, T, broadcast a message to the ad hoc group that unfold the revocation on the occasion that a certificate desires to be revoked. Calling the revoked certificate certr , the transmission look like as:

T → broadcast: [revoke, certr]PT − node that receiving this message rebroadcasts it to its neighbors. Revocation observes need to be stored until the revoked certificate would have expired normally. Any neighbor of the node needs to reform routing with the revoked certificate as necessary to avoid the untrusted transmission.

3. CLASSIFICATION OF AUTHENTICATION PROTOCOLS

Authentication protocols mentioned in the literature have introduced a variety of ways in which the authentication function may be carried out. Some protocols presuppose the existence of a third party that is trusted by all nodes. The trusted third party signifies a service whose signature on a requester's certificate is pondering a proof of its identity and is relied on to make authentication decisions. On the other hand, other protocols acknowledge no such service in the network. The first classification declares the different kind of certificate used for authentication. As stated earlier, a certificate is a unique identifier that can be used to authenticate a node with lofty definiteness. The Certificate may be classified into two categories. (1) Requester based on a unique custody (2) requester based on context. The second classification based on the roles referred to nodes in the network with respect to the authentication process. On the basis of that, authentication protocols can be categorized into two categories: homogeneous and heterogeneous.

The third classification b e l i e v e s on the fact that Some protocols set up certificate earlier to node deployment, on the other hand protocols acknowledge certificate are established post node deployment. A third prospective comes into existence, when some certificates are pre-dispense offline, but the actual certificate used for authentication derive from the pre-dispensed certificate. While other factors for classification are possible.

4. CLASSIFICATION BASED ON AUTHENTICATION FUNCTION

Homogeneity points out that all nodes in the network have the same role with respect to the authentication process. This category of authentication protocols acknowledge s that nodes in the network either make authentication judgment separately or they dangle on information give by other nodes in the network to make such choices under the reliant homogeneous class of authentication protocols, authenticators trust on information from their trusted peers to make authentication decisions. Trust based methods that use trust chains fall under this class. On the other hand, in the autonomous homogeneous class, authenticators make authentication decisions separately without trusting on their peers or any superimpose infrastructure. The use of convincing identification, identity based cryptography, and credit b a s e d m e c h a n i s m s s u c h as [27] is general among protocols in this class. In general, authentication protocols which follow the trust based mechanisms fall under the homogeneous class of authentication protocols ([15].Examples of schemes that fall under the homogeneous autonomous subclass are [1] [3] [25] [6] [8] [11] [13], while [2] [5] [32] [23] [9] [10] [18] [26] are schemes that fall under the homogeneous retainer subclass.

The heterogeneous class of protocols point out that nodes in the network have unusual roles with respect to the authentication process. This sign that there is an main service in the network that is intended to help other nodes in making authentication judgment (e.g., a trusted third party). The main service could be centralized, where one specialized node is accountable for giving that service, scattered, where service nodes are deployed anywhere in the network impedance to service desires from any node, or clustered. Each cluster has a unique contributor of the authentication service. Authentication protocols that are based on PKI or symmetric key fall under the heterogeneous authentication class. Examples of authentication scheme that fall under the heterogeneous centralized subclass is [14], while [4] & [24] are schemes that follow the heterogeneous clustered subclass. [16] & [17] are schemes that fall under the heterogeneous disseminated sub class.

5. CLASSIFICATION BASED ON TYPE OF CERTIFICATE

The Certificate can be classified into two classes: identity-based and context-based therefore the classification of authentication protocols based on the type of certificate used for authentication. This category identifies a unique protective hold by the requester that could be used to identify it with high certainty. The authenticator could be confident about the requester's identity if it is sure that the requester possesses that key. Identity based certificate can be advance into two subcategory one is encryption based and other is non-encryption based. An encryption based identity certificate is a portion of information generated and cryptographically signed with the key obsessed by the requester in order to verify its custody of the key, and consequently prove its identity. In order to verify the requester's identity, the authenticator must either hold the same key (symmetric key cryptography), or the public key part of the private-key hold by the requester (asymmetric key cryptography). In sensor networks the most common approach to achieve the authentication is symmetric key based authentication since it is less resource dependent as compared to asymmetric key. On the other hand, asymmetric key based authentication, or public key cryptography, have need of deployment of a public key infrastructure (PKI). Further we can say that, it requires the existence of a trusted authority whose task is to bind entities' identities to their public keys and release a signed certificate showing their authenticity .The service of such an authority must be obtainable anytime anywhere. One form of non-encryption based identity certificate is information that is hashed using a one-way key-based hash function and the key hold by the requester. . In order to verify the requester's identity, the authenticator must hold the same key (symmetric key) and the hashed information as the requester in order to re-generate the hash value and confirm the claimed identity of the requester. Another form of hash based non-encryption identity certificate uses delayed key disclosure as in TESLA. Another kind of identity-based certificate is a joint secret. A shared secret is not necessarily a key. Hence, it will not be applied as the basis for any cryptographic practice. One example is root administrators of greatly secure machines who create a file in the root directory to prove their identity to the authenticator. This is an operation allowed only to the administrator. Therefore, root confirms its identity without disclosing the password. The authenticator has to challenge the requester until the requester influence the authenticator that it knows that secret. This authentication method is called zero knowledge proofs and it can be used in ad hoc networks. Contextual based certificatecan be activities or physical. Activity-based contextual certificate go to identify and authenticate a requester based on its pattern of activities. In this method an authenticator would keep an eye on the activity pattern of the requester with respect to certain functionality and classify it based on its performance. On the other hand, physical-characteristics based contextual certificate attempt to identify and authenticate an influence the authentication process. furthermore, users 'mobility united with QoS and security requirements state the requirement of interaction between the different types of self-directed networks that may be used by mobile applications. If not accurately handled, the requester based on a physical characteristic that uniquely identifies it, such as its GPS location, RSSI (Received Signal Strength Indication), or SNR (Signal to Noise Ratio).This kind of certificate depend on the situation where the authentication procedure is performed. We divide this kind of certificate in two subclasses: activity related and physical data related certificate.

6. CLASSIFICATION BASED ON ESTABLISHMENT OF CERTIFICATE

The first type of authentication protocols under this classification believe in a pre-distribution offline phase (before deployment) where certificate are set up .Pre- deployment of certificate is commonly used in symmetric- key-based protocols in SensNets. The second type of authentication protocols believe in a post deployment phase , such as protocols that rely on contextual information. The third category, similar to the first one, believes in predistribution of initial certificate. Conversely, the actual certificate which is used for authentication is resulting from the initial certificate post deployment.

7. CONCLIONS AND OPEN R ESEARCH ISSUES

The sufficient security measures for ad hoc networks are a demanding task. Wireless communications are simple to catch and difficult to surround. This means that insecure wireless networks are open to a wide range of attacks, including message injection, loss of confidentiality, node impersonation, etc. In many states the nodes may be left unobtainable in a hostile environment. This entitles adversaries to detain them and physically attack them. Proper safety measures (tamper resistant) are required to prevent attackers from extracting secret information from them. Any security solution with a static arrangement would not be enough. Security mechanisms should be able to adapt on-the-fly to these changes in topology. Security mechanisms should be scalable to handle such a large network. We have presented a common authentication procedure and developed a classification of authentication protocols. This paper doesn't present the logic that would explain every authentication protocol but fairly provide a way through which classification has been done. Related open research issues include performance analysis of authentication protocols in variety of Ad-hoc application and protocol survivability in presence of different attacks.

8. REFERENCES

[1] S. Zhu, S. Xu, S. Setia and S. Jajodia, "LHAP: A lightweight hop-by-hop authentication protocol for ad- hoc networks." In Proc. of ICDCS 2003 International Workshop on Mobile and Wireless Network (MWN 2003), May 2003.

[2] A. Weimerskirch and G. Thonet, "A Distributed Light-Weight Authentication Model for Ad-hoc Networks." In Proc. of 4th International Conference on Information

Security and Cryptology (ICISC 2001), 6-7 December 2001.

[3] D. Balfanz, D. K. Smetters, P. Stewart and H. Chi. Wong, Talking to Strangers: Authentication in Ad- Hoc Wireless Networks." In Symposium on Network and Distributed Systems Security (NDSS '02).

[4] L. Venkatraman and D. Agrawal, "A Novel Authentication cheme for Ad Hoc Networks." In IEEE Wireless Communications and Networking Conference (WCNC 2000), vol. 3, pp. 1268--1273, 2000.

[5] H. Deng, A. Mukherjee, D. P. Agrawal, "Threshold and Identity-Based Key Management and Authentication for Wireless Ad Hoc Networks." International Conference on Information Technology: Coding and Computing (ITCC'04).

[6] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks." In 10th ACM Conference on Computer and Communications Security (CCS '03).

[7] D. Park, C. Boyd, E. Dawson. "Classification of Authentication Protocols: A Practical Approach." Proceedings of the Third International Workshop on Information Security.

[8] A Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, "SPINS: Security Protocols for Sensor Networks." In Proc. Of ACM Mobicom'01.

[9] Edith C. H. Ngai and Michael R. Lyu, "Trust- and Clustering- based Authentication Services in Mobile Ad Hoc Networks." In Proc. of 24th International Conference on Distributed Computing Systems Workshops - W4: MDC (ICDCSW'04).

[10] Edith C. H. Ngai and Michael R. Lyu and Roland T. Chin, "An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks." In Proc. of 2004 IEEE Aerospace Conference, March 6-13 2004.

[11] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks." In M. Roe B. Christianson, B. Crispo, editor, Security Protocols, 7th International Workshop Proceedings, LectureNotes in Computer Science. Springer Verlag, 1999.

[12] IEEE Std 802.11a-1999 Supplement to IEEE standard for information technology telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: high-speed physical layer in the 5 GHz band

[13] A. Weirmerskirch and D. Westhoff, "Identity Certified Authentication for Ad-hoc Networks." In Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003, VA USA.

[14] S. Gokhale and P. Dasgupta, "Distributed Authentication or Peer-to-Peer Networks", In Symposium on Applications and the Internet Workshops 2003 (SAINT'03 Workshops).

[15] R. Yahalom, B. Klein, Th. Beth, "Trust Relationships in Secure Systems- A Distributed Authentication Perspective." In Proc. of the 1993 IEEE Symposium on Security and Privacy,CA USA.

[16] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks." IEEE Network Journal, vol. 13, no. 6,1999, pp. 24-30.

[17] A. A. Pirzada, C. McDonald, "Kerberos Assisted Authentication in Mobile Ad hoc Networks." Proceedings of the 27th conference on Australasian computer science.

[18] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-Securing Ad Hoc Wireless Networks." In Seventh IEEE Symposium on Computers and Communications (ISCC '02),2002

[19] S. Hahm, Y. Jung, S. Yi, Y. Song, I. Chong, and K. Lim, "A Self-organized Authentication Architecture in Mobile Ad-hoc Networks." International Conference on Information Networking (ICOIN) 2005.

[20] Clark and J. Jacob, "A Survey of Authentication Protocol Literature: Version 1.0", 17 November 1997.

[21] S. Basagni and K. Herrin, "Secure pebblenets." In Proc. of the 2nd ACM international symposium on Mobile ad hoc networking & computing, 2001.

[22] A. Perrig, R. Canetti, J. Tygar, D. Song, "Efficient authentication and signing of multicast streams over lossy channels." In Proc. of IEEE Symposium on Security and Privacy, May 2000.

[23] Wenliang Du, RonghuaWang, and Peng Ning, "An Efficient Scheme for Authenticating Public Keys in Sensor Networks." In Proc. of 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005.

[24] M. Bechler, H.-J. Hof†, D. Kraft, F. Pählke, L. Wolf "A Cluster-Based Security Architecture for Ad Hoc Networks" INFOCOM 2004.

[25] J. Binder and H-P. Bischof, "Zero knowledge proofs of identity for ad hoc wireless networks."2003.

[26] A. Fritz and J.-F. Pâris, "Maille Authentication: A Novel Protocol for Distributed Authentication." In Proc. of the 19th IFIP Information Security Conference (SEC 2004), Toulouse, France, Aug. 2004, pages 309–322.

[27] M. Tamer Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy "A Reputation-based mechanism for Isolating Selfish Nodes in Ad Hoc networks". In Proc. of the IEEE Mobiquitous 2005, San Diego, CA.

[28] A. Aresenault and S. Turner, "Internet X.509 public key infrastructure," draft-ietf-pkix-roadmap-06.txt, 2000

[29] R. Perlman, "An overview of PKI trust models", IEEE Network, p. 38-43, vol.13, (no.6) Nov.-Dec. 1999

[30] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network, vol. 13, no. 6, pp. 24–30, 1999.

[31] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Net- works," in Proc. MobiCom, Aug. 2000.