Security in Ad Hoc Networks

Zheng Yan
Networking Laboratory
Helsinki University of Technology
zheng.yan@hut.fi

Abstract

This paper analyzes security challenges in ad hoc networks and summarizes key issues that should be solved for achieving the ad hoc security. It also gives an overview of the current state of solutions on such key issues as intrusion detection, secure routing and key management service. Based on our study, we present using external CA (Certificate Authority) and tamper-resistant chip to support ubiquitous security in the ad hoc environment. In our proposal, the external CA is involved into the ad hoc networks when necessary. It can also be used to broadcast blacklist and shared-password to normal nodes by deploying broadcast encryption. The tamper-resistant chip can be embedded into the ad hoc node device to support secure storage, high secure session key generation, secure communication and secure data processing based on usage and access control information embedded by the data source. They can also support or cooperate with other existed ad hoc security mechanisms.

1 Introduction

Ad hoc networks are new paradigm of networks offering unrestricted mobility without any underlying infrastructure. An ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner. In the ad hoc networks, there is no fixed infrastructure such as base station or mobile switching. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than in a wired network. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes.

There are two major types of wireless ad hoc networks: Mobile Ad Hoc Networks (MANETs) and Smart Sensor Networks (SSNs). A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activities including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. Significant applications of MANETs include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks which cannot rely on centralized and organized connectivity. A smart sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and sufficient intelligence for signal processing and networking. Some examples of smart sensor networks are the following: Military sensor networks to detect enemy movements, the presence of hazardous material. Environmental sensor networks to detect and monitor environmental changes. Wireless traffic sensor networks to monitor vehicle traffic on a highway or in a congested part of a city. Wireless surveillance sensor networks for providing security in a shopping mall, parking garage, or other facility. Wireless parking lot sensor networks to determine which spots are occupied and which spots are free. In this paper, our discussion will mainly focus on the MANETs.

Military tactical operation is still the main application of ad hoc networks today. Simultaneously, since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses. Security is a very important issue for ad hoc networks, especially for security-sensitive applications. It is an essential component for basic network functions such as packet forwarding, routing and network management, which are carried out by all available nodes in the ad hoc networks. Due to the basic difference from the fixed networks, security in the ad hoc networks should be re-examined and re-considered. This paper aims to give an overview of the current state of the ad hoc security, to analyze its requirements and to discuss its challenges and technologies. We also present some secure methods for achieving security in the ad hoc networks.

2 Security analysis

In this section, we analyze the security in the ad hoc networks based on their idiosyncrasies.

2.1 Idiosyncrasies of Ad Hoc Networks

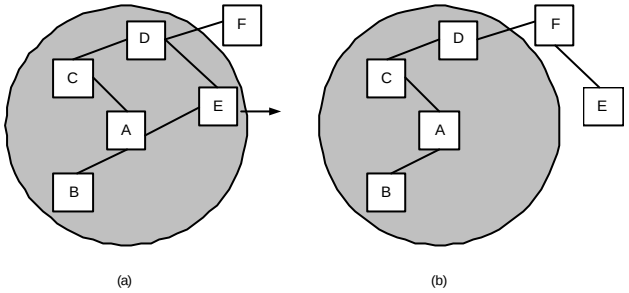

Figure 1: Topology changes in ad hoc networks

In the ad hoc networks, mobile nodes within each other's radio range communicate directly via wireless link using a protocol such as IEEE 802.11 [1] or Bluetooth [2], while those far apart rely on other nodes to relay messages as routers. Due to the mobility of the nodes, the network topology is frequently changed. Figure 1 shows an example. The original network topology is shown in (a) where node E is inside node A's radio range, therefore node A has a direct link with node E. When node E moves out of A's radio range, as shown in (b), the original direct link between A and E is broken. However, the link from A to E is still kept, because A can reach E through C, D, and F.

As can be seen from the above, the ad hoc networks are quite different from traditional, hardwired packet networks. In [3, 4], salient idiosyncrasies of the ad hoc networks are analyzed as the following.

- Dynamic topologies:

Node mobility causes the network topology--which is typically multihop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

- Bandwidth-constrained, variable capacity links:

Compared with hardwired counterparts, wireless links will continue to have significantly lower capacity. In addition, aggregate application demand will likely approach or exceed network capacity frequently. As the rapid extension of the traditional networks, similar services, such as multimedia commerce, are required to be supported by the ad hoc networks.

- Energy-constrained operation:

Most possibly, some or all of the nodes in an ad hoc network are actually mobile devices, which may rely on batteries or other exhaustible means for their energy. For these nodes, optimization for energy conservation is a critical design criterion.

- Wireless vulnerabilities and Limited physical security:

Operation in an ad hoc network introduces some new security problems in addition to the ones already present in fixed networks. Mobile wireless networks are generally more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of-service, and impersonation attacks is increased. Existing link security techniques are often applied within wireless networks to reduce security threats.

2.2 Security goals

Similar to the traditional networks, security of the ad hoc networks is considered from the following attributes.

- Availability

Availability requires that network assets are available to authorized parties when needed and ensures the survivability of network services despite denial-of-service (DOS) attacks, which could be launched at any layer of the ad hoc network. The DOS attack can cause physical jamming, disrupt routing protocol, disconnect the network and bring down high-level services, such as key management service, an essential service for any security framework.

- Confidentiality

Confidentiality ensures that certain information is never disclosed to unauthorized entities. In the ad hoc network, not only sensitive information transmitted requires confidentiality; routing information must also remain secure in case it might be valuable for adversaries.

- Integrity

Integrity guarantees that information being transferred is never altered. Only authorized nodes are able to modify the transferred information. Both malicious attacks and benign failure, such as radio propagation impairment could cause information corruption.

- Authentication

Authentication enables communication parties could identify with each other. Therefore, an adversary can not masquerade a node to gain sensitive resources.

- Nonrepudiation

Nonrepudiation guarantees that the information origin can not deny having sent the information. This is useful for detection and isolation of compromised nodes.

- Access and usage control

Access control makes sure that access to information resource is controlled by the ad hoc networks. Usage control ensures the information resource is used correctly by the authorized nodes having the corresponding rights. This mechanism provides the ability to control information after it is transmitted.

2.3 Challenges and key issues

The salient features of the ad hoc networks pose challenges in achieving the security goals.

First of all, the use of wireless link renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active interfering. Unlike fixed hardwired networks with physical defense at firewalls and gateways, attacks on an ad hoc network can come from all directions and target at any node. Damage can include leaking secret information, interfering message and impersonating nodes, thus violating the above security goals. All these mean that every node must be prepared for encounter with an adversary directly or indirectly.

Second, autonomous nodes in an ad hoc network have inadequate physical protection, and therefore more easily to be captured, compromised, and hijacked. We should consider malicious attacks launched from both outside and inside the network. Since it is difficult to track down a particular mobile node in a large scale of ad hoc network, attacks from a compromised node are more dangerous and much harder to detect. All these indicate that any node must be prepared to operate in a mode that trusts no peer.

Third, any security solution with static configuration would not be sufficient because of the dynamic topology of the networks. In order to achieve high availability, distributed architecture without central entities should be applied. This is because introducing any central entity into security solution may cause fatal attack on the entire network once the centralized entity is compromised. Generally, decision making in the ad hoc networks is decentralized and many ad hoc network algorithms rely on the cooperation of all nodes or partial nodes. But new type of attacks can be designed to break the cooperative algorithm. As can be seen from the above, no matter what security measures are deployed, there are always some vulnerability that can be exploited to break in.

Based on the above analysis, we further summarize three key issues for achieving the security of ad hoc networks.

- Intrusion detection

As we have known, the ad hoc networks are particularly vulnerable due to its features of dynamic changing topology, lack centralized monitoring and management point and lack of defense. Intrusion prevention measures, such as encryption and authentication, are required to protect network operation. But these measures can not defend compromised nodes, which carry their private keys. The ad hoc networks have inherent vulnerabilities that are not easily preventable. Intrusion detection presents a second wall of defense and it is a necessity in any high-availability network. But many of the intrusion detection techniques developed on a fixed hardwired network are not applicable in this new environment. How to detect intrusion differently and efficiently is a challenge.

- Secure routing

In the ad hoc networks, routing protocol should be robust against topology update and any kinds of attacks. Unlike fixed networks, routing information in an ad hoc network could become a target for adversaries to bring down the network. There are two kinds of threats to ad hoc routing protocols. The first one comes from external attackers. The attacks include injecting erroneous routing information, replaying old routing information, and distorting routing information. Using these ways, the attackers can successfully partition a network or introduce excessive traffic load into the network, therefore cause retransmission and ineffective routing. Using cryptographic schemes, such as encryption and digital signature can defend against the external attacks. The second threat comes from compromised nodes, which might send malicious routing information to other nodes. It is more severe because it is very difficult to detect such malicious information because compromised node can also generate valid signature.

Existing routing protocols cope well with the dynamic topology, but usually offer little or no security measures [5]. An extra challenge here is the implementation of the secured routing protocol in a network environment with dynamic topology, vulnerable nodes, limited computational abilities and strict power constrains.

- Key management service

Traditional cryptographic mechanisms, such as digital signature and public key encryption, still play vital roles in achieving security goals in the ad hoc networks. All these mechanisms require a key management service to keep track of key and node binding and assist the establishment of mutual trust between communication nodes. Traditionally, the key management service is based on a trusted entity called a certificate authority (CA) to issue public key certificate of every node. The trusted CA is required to be online in many cases to support public key revocation and renewal. But it is dangerous to set up a key management service using a single CA in an ad hoc network. As we have analyzed, the single CA will be the vulnerable point of the network. If the CA is compromised, the security of the entire network is crashed. How to set up a trusted key management service for the ad hoc network is also a big issue.

3 State of the art

In this section, we further study the current state of the above issues.

3.1 Intrusion detection

An intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability" [6]. Intrusion protection techniques work as

the first line of defense. However, intrusion protection alone is not sufficient because there is no perfect security in any network system, especially in the ad hoc networks. Intrusion detection can be used as the second line of protection to capture audit data and dig out evidence in the data to determine whether the system is under attack. Because once an intrusion is detected, e.g. in the early stage of a DDOS (Distributed Denial-of-Services), measures can be taken to minimize the damages, gather evidence for prosecution and even launch counter-attacks. This is very important in the ad hoc network to find compromised nodes promptly and take corresponding actions to against.

Generally speaking, intrusion detection system (IDS) can be classified as network-based or host-based according to the type of audit data used. A network-based IDS runs at the gateway of a network and captures and examines the packets going through it. This kind of IDS is not suitable for the ad hoc networks where there are no traffic concentration points. A host-based IDS relies on operating system audit data to monitor and analyze the events generated by programs or users on the node. In the ad hoc networks, the useful audit data at the node include system and user activities within the mobile node, communication activities by this node, as well as communication activities within the radio range and observation of the node.

The intrusion detection techniques can be categorized into misuse detection and anomaly detection. The misuse detection uses patterns of well-known attacks to match and identify known intrusions. It can accurately and efficiently detect instances of known attacks, but it lacks ability to find out newly invented attacks. In the ad hoc networks, it is more difficult to model the pattern of known attacks due to the complexity and mobility of the networks. The anomaly detection flags observed activities that deviate significantly from the established normal usage as possible intrusions. This detection does not require prior knowledge of intrusion and can thus detect new intrusions. The disadvantage is it may not be able to indicate what intrusion is and may have high false rate. Furthermore, there may not be a clear separation between normalcy and anomaly in the ad hoc networks. This model may not be suitable to deploy for the ad hoc environment.

A distributed and cooperative architecture for better intrusion detection was proposed in [6]. Based on the proposed architecture, a statistical anomaly detection approach is used and the detection is done locally in each node and possibly through cooperation with all nodes in the network via the data collected from other nodes. In authors' opinion, the intrusion detection should take place in all networking layers in an integrated cross-layer manner. But how to define the anomaly models based on what kinds of trace data for the ad hoc networks is a main challenge.

3.2 Secure routing

Ad Hoc routing protocols can be divided into three classes [18]. *Table-driven* or *proactive* protocols require the periodical refreshing or updating of the routing information so that every node can operate with consistent and up-to-date routing tables. The advantage of the proactive approach is that once a route is formed, its use is efficient. But the pure proactive protocols do not suite the ad-hoc networks due to the heavy routing information exchange. *Source-initiated on-demand driven* or *reactive* protocols, in contrary, do not periodically update the routing information - the data is propagated to the necessary nodes only when necessary. Many of the ad hoc protocols fall into this class. They create network traffic only when the routing fabric must really be changed. The disadvantage of the reactive protocols is that they create a lot of overhead when the route is being determined. The third class, *hybrid* protocols, make use of both approaches by adapting the protocol to the specific conditions. For instance, table-driven protocols could be used between networks and on-demand protocols inside the networks or vice versa. But few of them, to our knowledge, have security mechanism to defend against malicious attacks. In what follows, some solutions are presented.

TIARA

In [7], a set of design techniques for intrusion resistant ad hoc routing algorithm (TIARA) was presented mainly to against denial-of-service attacks. The TIARA design techniques include flow based route access control (FRAC), multi-path routing, flow monitoring, source-initiated router switching, fast authentication, sequence numbers and referral based resource allocation. These mechanisms can be used to against resource depletion attack, flow disruption attack and route hijacking. With the FRAC, each node holds an access control rule base (policies) that defines the list of authorized flows that can be forwarded by the node. The multi-path routing requires ad hoc routing algorithms should discover and maintain all legitimate routes for a data flow. In case one route (e.g. shortest route) is attacked, another safe route can be used. By making use of the source-initiated flow routing, the source can indicate which path is initiated by inserting the path label in each data package. For supporting the source-initiated flow routing, the flow monitoring is deployed to detect the failure of a path and to notify the source of the data flow. The fast authentication is proposed instead of traditional techniques used with IPSEC. It relies on placing the path label of a packet at a node specific secret location, and this secret location is conveyed to each routing node in a secure fashion by the route establish function of the ad

hoc routing algorithm. In addition, the sequence numbers provide a counter measure for replay attacks and the referral-based resource allocation mechanism help the routing node limit the maximum amount of network resources allocating for a flow.

The TIARA is routing algorithm independent. It can handle attacks on both routing traffic and data traffic. In order to implement it, existing ad hoc routing algorithm should be changed. Unfortunately, the paper did not indicate how to change the algorithms, especially how to realize fast authentication.

Secure aware ad hoc routing (SAR)

Secure aware ad hoc routing (SAR) in [18] introduces security properties as a negotiable metric to discover secure routes in an ad hoc network. Quality of protection offered by the discovered route directly affects the security of data packets exchanged between the nodes on a particular route. Routing information, such as route updates and route propagation messages, is also protected using this way. The security properties, such as time stamp, sequence number, authentication password or certificate, integrity, confidentiality, non-repudiation, etc. have a cost and performance penalty associated with it, therefore effect the secure route discovery.

The SAR can be implemented based on any on-demand ad hoc routing protocol with suitable modification. The security metric can be embedded into the RREQ packet with changed forwarding protocol. Intermediate nodes receive the RREQ packet with a particular security metric or trust level. The SAR ensures that these nodes can process the packet or forward it only if they can provide the required security or have the required authorization or trust level.

Lowering security overhead in link state routing

Some work is done to lower the traffic overhead caused by security protection. A mechanism is proposed in [15] for allowing the nodes to send substantially lighter routing information packets when the Link State Updates (LSU) would be redundant in respect of the previously exchanged information. The source node that sends the routing information to the other nodes applies a hash chain. The message includes a computation of $h(h(...(h(R))))$ of some randomly chosen data R, which is hashed N times. After the first original message, the origin node can then refresh the redundant routing information by sending the nodes the random data R hashed only $N - 1$ times. In this way the receiver nodes can refresh their routing information by computing the hash of the chain and verifying that the result is indeed equal to the original hash chain associated with the routing information that was authenticated within the first routing information exchange. After that, if the same routing information is still valid, the origin node sends a hash chain of $N - 2$ hashes and so on, until the number of hashes in the chain N is zero, in which case the routing information must be renewed totally.

This approach can substantially reduces the computational overhead, if the routing information is typically redundant, since hash functions are much faster compared to the digital signatures and other public-key methods. This method does not include any source routing approaches. In addition, the length of the hash chain is always the same; thus an adversary cannot find out the length of the chain by just inspecting it. On the other hand, in the dynamic ad hoc environment having the severe problems with compromised nodes, this approach seems to be inadequate. Because it is vulnerable when the source node is compromised and keeps the incorrect routing information by setting the hash chain to be very long.

3.3 Key management service

As discussed before, key management service is the basic issue on the ad hoc security if traditional cryptographic way is deployed. The most popular ideas today are introduced below.

Key agreement

In [12], Asokan and Ginzboorg presented a new protocol for password-based multi-party key agreement in an ad hoc scenario that a group people in a meeting room do not have access to public key infrastructure or third party key management service, but need to set up a secure session among their computers. The protocol illustrates Diffie Hellman key exchange based on shared password authentication between two parties and among multiple parties. It derives a strong-shared session key from the weak shared password. Key agreement is a fundamental building block for various security services. But this protocol is only suitable for the above special scenario. A password has to be shared by all the nodes involved in the ad hoc network. The authors do not consider how to renew the password in case some nodes leave or are compromised.

Threshold cryptography

In [5] and [8], threshold cryptography is used to provide robust and ubiquitous security support for the ad hoc networks. The basic idea is the CA functions are distributed through a threshold secret sharing mechanism, in which each entity holds a secret share and multiple entities jointly provide complete services. In the proposed designs for an ad hoc network with totally N nodes, K nodes hold secret share of the CA's private key, K nodes jointly can provide a complete CA signature. The system security can not be compromised as long as

there are less than *K* share holders to be broken. That is an adversary must destroy (*N-K+1*) nodes in order to turn off certification services. To further resist intrusions, the secret shares are updated periodically.

As can be seen from the above, the system security depends on the total number of share holders (*K*). If *K = 1*, it is the case of centralized solution, which is totally vulnerable based on the previous analysis. If *K = N*, the system security is lost once any single node is attacked, which is also vulnerable and unscalable. At least *N = 3*K + 1* is suggested in [5] to maintain the adequate security level and trust relationship. But it is questionable whether this threshold is adequate enough in different ad hoc environment. On the other hand, how to re-establish the secret shares in selected K nodes is also a problem in case that *K* or *K* selected nodes has to be changed due to dynamic topology, or compromised share holders, etc. Missing centralized network management in the ad hoc environment makes this very difficult to realize.

4 Proposals

Current academic research on the ad hoc security mainly focuses on some specific aspects with some assumption. There is no solution proposed that is really practical. In this part, we propose some idea for achieving the security in the ad hoc networks.

4.1 External CA

Since distributing CA functions through a threshold secret sharing mechanism is not practical and applying centralized CA in the ad hoc networks is really vulnerable, we introduce an external CA which is involved into the networks when necessary.

Before the ad hoc network is set up, the external CA can issue public key pair and its certificate to every node and publish its public key. Based on the authorized certificates, trust can be built among the ad hoc nodes. The external CA can also be used to collect intrusion detection reports and make intrusion decision. In case some nodes are compromised, the external CA joins the network to broadcast the blacklist (compromised note list) and new shared-password (refer to 4.2) to the normal nodes. The external CA broadcasting can be based on broadcast encryption technology, such as [20]. It is a scheme that addresses the case when an authority broadcasts some valuable information and it is required that only legitimated clients should be able to decrypt the information. It also has quite efficient ways to trace down the traitor who has constructed new decryption. Broadcast encryption can also be used at key revocation, and key renewal, besides the main effect of node authentication. The broadcast encryption root key is generated securely by the external CA and its child keys are issued to the nodes when their public key certificates are issued. When the information is broadcast, the external CA encrypts the information using the root key and decides which child keys can be used to decrypt it.

The external CA can be set up at a satellite or a group of satellites or a flight. There are two ways to initiate the communication between the external CA and the ad hoc nodes.

- On-demand

When emergency happens, e.g. intrusion detected locally, nodes leaving, etc, one node or a number of nodes request the external CA to report intrusion or anomaly, and to reissue shared-password.

- Time-based

The external CA periodically contacts the nodes, collects intrusion reports and reissues shared-password if necessary. The concrete time can be decided by the external CA, therefore it is hard for the adversary to interrupt the communication.

This idea is suitable for military tactical operations. It can also be tailored for other ad hoc applications. It has advantage that the external CA is not easy to be broken, thus it is more secure to realize any mechanism for secure routing, intrusion detection and data communication. In addition, the external CA only appears if it is needed, thus save the communication cost.

4.2 Tamper-resistant ad hoc chip

The external CA solves the root trust of the ad hoc networks. But in order to achieve the security goals, every ad hoc node device should have mechanisms to protect from various attacks. We propose a tamper-resistant ad hoc chip, which can be embedded into any ad hoc compatible device to support the external CA based security solution.

The proposed chip has the following features:

1. It is broken once it is attacked, any data save in the chip is erased.
2. A secure memory for saving confidential data, e.g. node private key, the external CA's child-key of that node and shared-password announced by the CA, as well as the blacklist.
3. A mechanism to generate high secure session key based on the shared-password. The session key can be used for data encryption. Based on the shared-password, any node can calculate the same session key by itself. In case of high security requirement, the session key can be negotiated according to [12].
4. A mechanism to decrypt data and process it in the local memory, ensure that any secure data saved in out-chip memory are in the encryption format.
5. A mechanism to realize fast authentication (3.2) by calculating the secret location in a packet based on node ID (or node public key) and the shared-password.

6. A mechanism to find the secret location and parse / process the data at that location. The data at the secret location not only include the path label, but also bind usage and access control information, as well as the metadata of the packet. The chip process the data based on the control information. E.g. the node device can only transfer the packet to its neighbor node if the packet's control data indicate it.
7. Secure communication with the external CA and other nodes through the broadcast encryption and public key encryption, as well as digital signature.

The advantages of the tamper-resistant ad hoc chip are:

- Highly secure: It is impossible to be attacked and get to know the data saved in its tamper-resistant memory.
- Flexible: It can support any ad hoc security solution based on some shared secret. What is more, it can also support solutions based on public key infrastructure. Any mechanism overviewed in the section 3 can be supported or cooperated with.
- Practical: it is implementable based on current technologies. The chip price will be going down quickly due to the fast development of chip processing ability.

5 Conclusion

This paper analyzed the security challenges in the ad hoc networks. We summarized three key issues that should be firstly solved for achieving the ad hoc security. Further more, we gave an overview of the current state of solutions on intrusion detection, secure routing and key management service respectively. We notified that security study in the ad hoc networks is just at the beginning period. Current achievement has weak points here and there. There is no solution that is really practical.

Based on our study, we proposed the external CA to solve the root trust problem in the ad hoc environment. The external CA is involved into the ad hoc networks if necessary and broadcasts the blacklist and shared-password to normal nodes by using the broadcast encryption. In order to support the external CA and other ad hoc security mechanisms, a tamper-resistant ad hoc chip was presented to support secure storage, high secure session key generation, secure data communication and secure data processing based on usage and access control information embedded by the data source. Our idea has the advantages of high security, flexibility and practicability. It can be treated as base-bone to support the security in the ad hoc networks.

References

[1] IEEE Wireless Local Area Networks, <http://www.ieee802.org/11/>

[2] Official Bluetooth Website, <http://www.bluetooth.com/>

[3] S. Corson, J. Macker: Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, 1999, <ftp://ftp.funet.fi/pub/standards/RFC/rfc2501.txt>

[4] S. Corson, J. Macker, G. Cirincione: Internet-Based Mobile Ad Hoc Networking, IEEE Internet Computing, Jul/Aug 1999.

[5] L. Zhou, Z. J. Haas: Securing Ad HocNetworks, IEEE Network, 13(6): 24-30, Nov/Dec 1999.

[6] Yongguang Zhang, Wenke Lee: Intrusion Detection in Wireless Ad-Hoc Networks, Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6-11 Aug. 2000.

[7] Ramanujan-R, Ahamad-A; Bonney-J, Hagelstrom-R, Thurber-K: Techniques for intrusion-resistant ad hoc routing algorithms (TIARA), Proceedings of IEEE Military Communications Conference (MILCOM'00), vol.2, Los Angeles, CA, USA, 22-25 Oct. 2000.

[8] Jiejun-K, Petros-Z, Haiyun-Luo, Songwu-Lu, Lixia-Zhang: Providing robust and ubiquitous security support for mobile ad-hoc networks, Proceedings Ninth International Conference on Network Protocols. ICNP 2001, Riverside, CA, USA, 11-14 Nov. 2001.

[9] Venkatraman-L, Agrawal-D-P: A novel authentication scheme for ad hoc networks, Proceedings of IEEE Conference on Wireless Communications and Networking, vol.3, Chicago, IL, USA, 23-28 Sept. 2000.

[10] Feeney-L-M, Ahlgren-B, Westerlund-A: Spontaneous networking: an application oriented approach to ad hoc networking, IEEE-Communications-Magazine (USA), vol.39, no.6, p.176-81, June 2001.

[11] Blazevic-L, Buttyan-L, Capkun-S, Giordano-S, Hubaux-J-P, Le-Boudec-J-Y: Self organization in mobile ad hoc networks: the approach of Terminodes, IEEE-Communications-Magazine (USA), vol.39, no.6, p.166-74, June 2001.

[12] Asokan-N, Ginzboorg-P: Key agreement in ad hoc networks, Computer Communications (Netherlands), vol.23, no.17, p.1627-37, 1 Nov. 2000.

[13] Gehrmann-C, Nikander-P: Securing ad hoc services, a Jini view, Proceedings of First Annual Workshop on Mobile Ad Hoc Networking Computing. MobiHOC Mobile Ad Hoc Networking and Computing, Boston, MA, USA, 11 Aug. 2000.

[14] Wenli-Chen, Nitin-Jain, Singh-S: ANMP: ad hoc network management protocol, IEEE-Journal-on-Selected-Areas-in-Communications (USA), vol.17, no.8, p.1506-31, Aug. 1999.

[15] Hauser-R, Przygienda-T, Tsudik-G: Lowering security overhead in link state routing, Computer-

Networks (Netherlands), vol.31, no.8, p.885-94, 23 April 1999.
[16] Seung Yi, Prasad Naldurg, Robin Kravet: Security-aware ad hoc routing for wireless networks, <http://www.cs.uiuc.edu/Dienst/Repository/2.0/Body/ncstrl.uiuc_cs/UIUCDCS-R-2001-2241/pdf>
[17] Silja Mäki: Security Fundamentals in Ad-hoc Networking, May, 2000, <http://www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/security_fund/internetworking.html>
[18] Vesa Kärpijoki: Signalling and Routing Security in Mobile and Ad-hoc Networks, May, 2000, < http://www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/signalling_security/index.html >.
[19] Harri Hansén: IPsec and Mobile-IP in Mobile Ad Hoc Networking, April, 2000, < http://www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/IPsec/index.html>.
[20] Yoshida, M., Fujiwara, T.: An efficient traitor tracing scheme for broadcast encryption, 2000 IEEE International Symposium on Information Theory, p.463.