Security in Ad Hoc Networks

Vesa Kärpijoki
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
Vesa.Karpijoki@hut.fi

Abstract

In ad hoc networks the communicating nodes do not necessarily rely on a fixed infrastructure, which sets new challenges for the necessary security architecture they apply. In addition, as ad hoc networks are often designed for specific environments and may have to operate with full availability even in difficult conditions, security solutions applied in more traditional networks may not directly be suitable for protecting them. A short literature study over papers on ad hoc networking shows that many of the new generation ad hoc networking proposals are not yet able to address the security problems and they face. Environment-specific implications on the required approaches in implementing security in such dynamically changing networks have not yet fully realized.

1 Introduction

An ad hoc network is a collection of *nodes* that do not need to rely on a *predefined infrastructure* to keep the network connected. Ad hoc networks can be formed, merged together or partitioned into separate networks on the fly, without necessarily relying on a fixed infrastructure to manage the operation. Nodes of ad hoc networks are often *mobile*, which also implicates that they apply *wireless* communication to maintain the connectivity, in which case the networks are called as *mobile ad hoc networks* (*MANET*). Mobility is not, however, a requirement for nodes in ad hoc networks, in ad hoc networks there may exist static and wired nodes, which may make use of services offered by fixed infrastructure.

Ad hoc networks may be very different from each other, depending on the area of application: For instance in a computer science classroom an ad hoc network could be formed between students' PDAs and the workstation of the teacher. In another scenario a group of soldiers is operating in a hostile environment, trying to keep their presence and mission totally unknown from the viewpoint of the enemy. The soldiers in the group work carry wearable communication devices that are able to eavesdrop the communication between enemy units, shut down hostile devices, divert the hostile traffic arbitrarily or impersonate themselves as the hostile parties. As can obviously be seen, these two scenarios of ad-hoc networking are very different from each other in many ways: In the first scenario the mobile devices need to work only in a safe and friendly environment where the networking conditions is predictable. Thus no special security requirements are needed. On the other hand, in the second and rather extreme scenario the devices operate in an extremely

hostile and demanding environment, in which the protection of the communication and the mere availability and operation of the network are both very vulnerable without strong protection.

As ad hoc networking somewhat varies from the more traditional approaches, the security aspects that are valid in the networks of the past are not fully applicable in ad hoc networks. While the basic security requirements such as confidentiality and authenticity remain, the ad hoc networking approach somewhat restricts the set of feasible security mechanisms to be used, as the level of security and on the other hand performance are always somewhat related to each other. The performance of nodes in ad hoc networks is critical, since the amount of available power for excessive calculation and radio transmission are constrained, as discussed e.g. in [3]. In addition, the available bandwidth and radio frequencies may be heavily restricted and may vary rapidly. Finally, as the amount of available memory and CPU power is typically small, the implementation of strong protection for ad hoc networks is non-trivial.

The main objective of this paper is to give an overview of how the area of application affects the security requirements of ad hoc networks. The focus of the discussion is in the security of routing. From the requirements criteria for evaluating existing ad hoc networking solutions are formed. The evaluated proposals include the contemporary MANET drafts of the IETF. Mobile IP is not discussed.

The paper is structured into six sections as follows. *Section 1* introduces the reader to the background of the topic: ad hoc networks and their special characteristics. *Section 2* concentrates on giving an overview of characteristics and areas of networking that are relevant when designing security architecture for ad hoc networks. *Section 3* discusses security aspects and requirements of ad hoc networks from the viewpoint of the categories presented in section 2. *Section 4* presents security problems encountered when the traditional networking approaches are applied in ad hoc networking. *Section 5* gives an overview of the contemporary solutions for the ad hoc networking and discusses the applicability of their security architecture. Finally, *section 6* proposes future work possibilities for securing ad hoc networks.

2 Networking

2.1 Networking Infrastructure

Networking infrastructure forms the basis for the networks on top of which the higher-level services can be built. The core of the networking infrastructure is formed by the *physical* topology and the *logical structure* of the network, of which the latter is implemented and maintained with *routing*. As discussed in [5], there are two approaches in networking:

- *flat* or *"zero-tier"* infrastructure
- *hierarchical*, *multiple-* or *N-tier* infrastructure.

In flat networks there are no hierarchies of nodes; all nodes have equivalent roles from the viewpoint of routing. In contrary, in hierarchical networks there are nodes that have differ-

ent roles than the others. These *cluster nodes* are responsible for serving one *cluster* of the actual low-tier nodes by controlling the traffic between the cluster and other clusters. Finally, the logical and physical topology of the network need not directly correspond to each other; for instance a *logically* hierarchical *routing fabric* can be formed with *physically* flat network topology and vice versa.

2.2 Networking Operations

Most important *networking operations* include *routing* and *network management*.

Routing protocols can be divided into *proactive*, *reactive* and *hybrid* protocols, depending on the routing topology [14].

- *Proactive* protocols are typically table-driven and distance-vector protocols, thus resembling many traditional protocols. In proactive protocols the nodes periodically refresh of the existing routing information so that every node can immediately operate with consistent and up-to-date routing tables whenever there is data to be sent. The pure proactive protocols do not suite ad hoc networks due to constant and heavy control traffic delivery between the nodes. Especially in MANET networks there often needs to exist several alternate paths to the destination for reliability reasons, which causes frequent exchange of redundant control information.
- *Reactive* or *source-initiated on-demand* protocols, in contrary, do not periodically update the routing information - it is propagated to the nodes only when necessary. Many of the MANET routing protocols are on-demand driven for optimization purposes The disadvantage of the reactive protocols is that they create a lot of overhead when the route is being determined, since the routes are not necessarily up-to-date when required.
- *Hybrid* protocols make use of both reactive and proactive approaches. They typically offer means to switch dynamically between the reactive and proactive parts of the protocol. For instance, table-driven protocols could be used between networks and on-demand protocols inside the networks or vice versa. It seems that networks neither the pure proactive nor the reactive approach is sufficient, due to the mentioned problems, so the hybrid approach may be in general the optimal choice.

The protection of routing traffic is vital in insecure environments so that the identity or location of the communicating party is not revealed to unauthorized parties. Routing information must also be protected from attacks against authentication and non-repudiation so that the origin of the data can be verified.

Network management involves the *configuration* of the elements in the network such as clients, routers and key management servers. The management can be done either *manually* or *automatically*, depending on the case. In addition to the initial configuration of the network as it starts, network management most often also involves the exchange and use of dynamic configuration information and status data of the network while operating. Network management data, as any piece of vulnerable information, must be protected from the viewpoint of confidentiality, authenticity and non-repudiation whenever the network is managed in a non-secure domain.

2.3 Physical Security

Physical security of the network elements forms the basis for the security architecture in networking. Moreover, the principles of the networking approach highly affect the importance and implications of the physical security. For instance, in web-based intranets of today the firewalls, proxies and any other centralized elements between the secure and non-secure domains are single points of failure, thus the physical security of such elements must be ensured. On the other hand, in the classroom example in the introduction, the physical security of the students' and teacher's devices is not an essential issue to be guaranteed. The exposure of a student's information may only break the privacy of a single user, not the whole network as in the previous intranet example. In centralized systems like in the classroom scenario the physical security of client nodes is thus not necessarily a critical issue, as the security of the system relies on the protection of a centralized service.

2.4 Key Management

The security in networking is in many cases dependent on proper *key management*. Key management consists of various services, of which each is vital for the security of the networking systems. The services must provide solutions to be able to answer the following questions:

- *Trust model*: it must be determined how much different elements in the network can trust each other. The environment and area of application of the network greatly affects the required trust model. Consequently, the trust relationships between network elements affects the way the key management system is constructed in network.
- *Cryptosystems*: available for the key management: in some cases only public- or symmetric key mechanisms can be applied, while in other contexts *Elliptic Curve Cryptosystems* (*ECC*) are available. While public-key cryptography offers more convenience (e.g. by well-known digital signature schemes), public-key cryptosystems are significantly slower than their secret-key counterparts when similar level of security is needed. On the contrary, secret-key systems offer less functionality and suffer more from problems in e.g. key distribution. ECC cryptosystems are a newer field of cryptography in terms of implementations, but they are already in use widely, for instance in smart card systems.
- *Key creation*: it must be determined which parties are allowed to generate keys to themselves or other parties and what kind of keys.
- *Key storage*: in ad-hoc networks there may not be a centralized storage for keys. Neither there may be replicated storage available for fault tolerance. In ad-hoc networks any network element may have to store its own key and possibly keys of other elements as well. Moreover, in some proposals such as in [19], *shared secrets* are applied to distribute the parts of keys to several nodes. In such systems the compromising of a single node does not yet compromise the secret keys.
- *Key distribution*: the key management service must ensure that the generated keys are securely distributed to their owners. Any key that must be kept secret has to be

distributed so that confidentiality, authenticity and integrity are not violated. For instance whenever symmetric keys are applied, both or all of the parties involved must receive the key securely. In public-key cryptography the key distribution mechanism must guarantee that private keys are delivered only to authorized parties. The distribution of public keys need not preserve confidentiality, but the integrity and authenticity of the keys must still be ensured.

2.5 Availability

In [19], *availability* is defined as one of the key attributes related to the security of networks. Availability guarantees that network services operate properly and tolerate failures, even when denial of service attacks threat the system. Availability can be broken in several layers: in the network layer the attacker can modify the routing protocol e.g. to be able to divert the traffic to invalid addresses or shut down networks. In session security management level the adversary may be able to unnoticeably remove encryption in the session-level secure channel. Finally, in application level the availability of the essential services such as key management service may be threatened.

2.6 Access Control

Access control consists of the means to govern the way the users or virtual users such as operating system processes (*subjects*) can have accesses to data (*objects*). In networking, access control can e.g. involve the mechanisms with which the formation of groups of nodes is controlled. Only authorized nodes may form, destroy, join or leave groups. Access control can also mean the way the nodes log into the networking system to be able to communicate with other nodes when initially entering the network.

There are various approaches to the access control: *Discretionary Access Control* (*DAC*) offers the means for defining the access control to the users themselves. DAC allows the restriction of access to objects based on the identity of subjects or groups of subjects. *Mandatory Access Control* (*MAC*) involves centralized mechanisms to control the access to objects with formal authorization policy. DAC and MAC are often applied together so that DAC allows the system user subjects to control access of other subjects, while MAC controls and restricts the operation of DACs in the system in general. This kind of approach prevents the system from failures generated by the actions of careless users.

Finally, *Role Based Access Control* (*RBAC*) applies the concept of *roles* within the subjects and objects. In RBAC systems subjects can have several roles of which one is at a time active and therefore the accesses to objects are defined with respect to roles, not subjects. As stated in [4], RBAC does not necessarily involve the controlling of access to information only, but also the restriction of access to *functions* within the system. Thus roles are group-oriented sets of *transactions* associated to roles that the specific users can perform to given objects. For example, in banking applications using RBAC users with different roles may have the same set of accesses to the same objects as such, only with different limits in the amount of transferable money. In DAC and MAC systems these kind of definitions could not be directly be applied.

3 Criteria for Protecting Ad Hoc Networks

3.1 Physical Security

In ad hoc networks especially mobile nodes are typically significantly more susceptible to physical attacks than wired nodes in traditional networks. However, the significance of the physical security in the overall protection of the network is highly dependent on the ad hoc networking approach and the environment in which the nodes operate. For instance in ad hoc networks that consist of independent nodes and work in a hostile battlefield the physical security of single nodes may be severely threatened. Therefore in such scenarios the protection of nodes cannot rely on physical security. In contrary, in the classroom example scenario the physical security of a node is an important issue to the owner of the node, perhaps for privacy reasons, but the breaking of the physical security does not affect the security of the system as such.

3.2 Security of Network Operations

The security of ad hoc networks can be based on protection in the *link* or *network layer*. In some ad-hoc solutions, the link layer offers strong security services for protecting confidentiality and authenticity, in which case all of the security requirements need not be addressed in the network or upper layers. For instance in some *wireless LANs* link layer encryption is applied. However in most cases the security services are implemented in higher layers, for instance in network layer, since many ad hoc networks apply IP-based routing and recommend or suggest the use of IPSec.

Most MANET routing protocols seem to handle the rapid changes to the networking environment rather well, as stated in [19]. As the routing protocol is responsible for specifying and maintaining the necessary *routing fabric* for the nodes, the protocol must be protected from any attack against confidentiality, authenticity, integrity, non-repudiation and availability. If confidentiality of the routing information is threatened, the adversary could be able to identify or locate nodes by eavesdropping the routing traffic they send and forward. For military applications the confidentiality is one of the most important attribute, as discussed in e.g. [6], since without the protection of location, identity and communication the users of the ad hoc network are very vulnerable to all kinds of attacks. On the other hand, if availability of the network is broken, the users may not be able to carry out their mission at all, as the communication links are broken or compromised.

Authenticity and integrity of routing information are often handled in parallel, if public-key cryptosystems are in use, since digital signatures are applied for both confirming the origin of the data and its integrity. Without any integrity protection the attacker is able to destroy messages, manipulate packet headers or even generate false traffic so that the actions cannot be distinguished from hardware or network failures. Authenticity of the routing data is essential so that nodes can confirm the source of new or changed routing information. If authenticity is not guaranteed, the adversary could perform impersonation attacks, divert traffic to arbitrary destinations or even scramble the routing fabric so that connectivity is severely broken in the ad hoc network. In worst case the attacker can perform his actions and leave the network without being regarded as a malicious party.

Non-repudiation is somewhat related to authenticity: routing traffic must leave traces so that any party sending routing information cannot later deny of having propagated the data to other parts of the network.

Network management data has similar security requirements as the routing traffic: the management information must be protected from disclosure, if it can contain vulnerable information such as status data that the nodes collect. The protection of management traffic against tampering and impersonation attacks is perhaps even more important. For example, if the status information the nodes send to the management system is not authenticated or protected against integrity attacks, a malicious node could capture the valid information and send invalid status data instead. This may lead to wrong assumptions about the condition of the nodes within the management system and lead to the use of invalid configuration data, as a reaction to the observed changes to statuses of nodes. Obviously, the impersonation attacks against the exchanged configuration information may have severe and unpredictable consequences - especially if the adversary can at the same time control the sending of status information from the nodes. Moreover, as in ad hoc networks the manual configuration of nodes may be impossible, the configuration data may have to be exchanged dynamically and on-demand, thus making the management operations even more vulnerable to the discussed attacks. In the worst case the adversary can arbitrarily configure any node and thus control the management system, which may interpret the observed inconsistencies as "natural" failures, not malicious actions generated by an active attacker.

3.3 Service Aspects

Ad hoc networks may apply either hierarchical or flat infrastructure both in logical and physical layers independently. As in some flat ad hoc networks the connectivity is maintained directly by the nodes themselves, the network cannot rely on any kind of *centralized* services. In such networks the necessary services such as the routing of packets and key management have to be *distributed* so that all nodes have responsibility in providing the service. As there are no dedicated server nodes, any node may be able to provide the necessary service to another. Moreover, if a tolerable amount of nodes in the ad hoc network crash or leave the network, this does not break the availability of the services. Finally, the protection of services against *denial of service* is in theory impossible. In ad hoc networks *redundancies* in the communication channels can increase the possibility that each node can receive proper routing information. Such approaches do, however, produce more overhead both in computation resources and network traffic. The redundancies in the communication paths, however, may reduce the denial of service threat and allow the system to detect malicious nodes from performing malicious actions more easily than in service provisioning approaches that rely on single paths between the source and destination.

Availability is a central issue in ad hoc networks that must operate in dynamic and unpredictable conditions. The network nodes may be idle or even be shut down once for a while. Thus the ad hoc network cannot make any assumptions about availability of specific nodes at any given time. For commercial applications using ad hoc networks availability is often the most important issue from the viewpoint of the clients. The routing protocol must guarantee the *robustness* of the routing fabric so that the connectivity of the network is maintained even when threatened by rapid changes in topology or attackers. Similarly,

in the higher layers, the services must be able to rely on that the lower layers maintain the packet-forwarding services at any time. Finally, many ad hoc networking protocols are applied in conditions where the topology must *scale up and down efficiently*, e.g. due to network partitions or merges. The scalability requirements also directly affect the scalability requirements targeted to various security services such as key management. In networks where the area of application restricts the possible size of the network, assumptions can be made about the scalability requirements of the security services as well.

3.4 Security of Key Management

As in any distributed system, in ad hoc networks the security is based on the use of a proper key management system. As ad hoc networks significantly vary from each other in many respects, an environment-specific and efficient key management system is needed. To be able to protect nodes e.g. against eavesdropping by using encryption, the nodes must have made a mutual agreement on a shared secret or exchanged public keys. For very rapidly changing ad hoc networks the exchange of encryption keys may have to be addressed on-demand, thus without assumptions about a priori negotiated secrets. In less dynamic environments like in the classroom example above, the keys may be mutually agreed proactively or even configured manually (if encryption is even needed).

If public-key cryptography is applied, the whole protection mechanism relies on the security of the private key. Consequently, as the physical security of nodes may be poor, private keys have to be stored in the nodes confidentially, for instance encrypted with a system key. For dynamic ad hoc networks this is not a wanted feature and thus the security of the private key must be guaranteed with proper hardware protection (smart cards) or by distributing the key in parts to several nodes. Hardware protection is, however, never alone an adequate solution for preventing attacks as such. In ad hoc networks a centralized approach in key management may not be an available option, as there may not exist any centralized resources. Moreover, centralized approaches are vulnerable as single point of failures. The mechanical replication of the private keys or other information is an inadequate protection approach, since e.g. the private keys of the nodes simply have then a multiple possibility to be compromised. Thus a *distributed approach* in key management - for any cryptosystem in use - is needed, as proposed e.g. in [19].

3.5 Access Control

The access control is an applicable concept also within ad hoc networking, as there usually exist a need for controlling the access to the network and to the services it provides. Moreover, as the networking approach may allow or require the forming of *groups* in for instance network layer, several access control mechanisms working in parallel may be needed. In the network layer the routing protocol must guarantee that no authorized nodes are allowed to join the network or a *packet forwarding group* such as the clusters in the hierarchical routing approach. For example in the battlefield example of the introduction the routing protocol the ad hoc network applies must control so that no hostile node can join and leave the group undetectable from the viewpoint of the other nodes in the group. In application level the access control mechanism must guarantee that unauthorized parties cannot have accesses to services, for instance the vital key management service.

Access control is often related to the *identification* and *authentication*. The main issue in the identification and authentication is that the parties can be confirmed to be authorized to gain the access. In some systems, however, identification or authentication of nodes is not required: nodes may be given e.g. delegate certificates with which the nodes can gain access to services. In this case actual authentication mechanisms are not needed, if the nodes are able to present adequate credentials to the access control system. In some ad hoc networks services may be centralized, while in other networks they are applied in a distributed manner, which may require the use of different access control mechanisms. Moreover, the required security level in access control also affects the way the access control must be implemented. If a centralized ad hoc networking approach with low security requirements is applied - as in the classroom example - the access control can be managed by the server party with simple means such as user id - password scheme. In ad hoc networks that operate in more difficult conditions without any centralized resources as in the battlefield scenario, the implementation of access control is much more difficult. Either the access to the network, its groups and resources must be defined when the network is formed, which is very inflexible. The other possibility is to define and use a very complex, scalable and dynamic access control protocol, which brings flexibility but is prone to various kinds of attacks and it may even be impossible to apply properly and efficiently.

4 Security Threats in Ad Hoc Networks

4.1 Types of Attacks

Attacks against ad hoc networks can be divided into two groups: *Passive attacks* typically involve only *eavesdropping* of data. *Active attacks* involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data. *External attacks* are typically active attacks that are targeted e.g. to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on. *Internal attacks* are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer. Thus such malicious insiders who may even operate in a group may use the standard security means to actually *protect their attacks*. These kind of malicious parties are called *compromised nodes*, as their actions compromise the security of the whole ad hoc network.

4.2 Denial of Service

The *denial of service* threat either produced by an unintentional failure or malicious action, forms a severe security risk in any distributed system. The consequences of such attacks, however, depend on the area of application of the ad hoc network: In the classroom example any of the nodes, either the teacher's centralized device or the students' handheld gadgets, can crash or be shut down without completely destroying anything - the class can continue their work normally by using other tools. On the contrary, in the battlefield scenario the efficient operation of the soldiers may totally depend on the proper operation of

the ad hoc network their devices have formed. If the enemy can shut down the network, the group may be separated into vulnerable units that cannot communicate with each other or to the headquarters.

The denial of service attack has many forms: the classical way is to flood any centralized resource so that it no longer operates correctly or crashes, but in ad hoc networks this may not be an applicable approach due to the distribution of responsibility. Distributed denial of service attack is a more severe threat: if the attackers have enough computing power and bandwidth to operate with, smaller ad hoc networks can be crashed or congested rather easily. There are however more serious threats to ad hoc networks: As discussed in e.g. [9], compromised nodes may be able to reconfigure the routing protocol or any part of it so that they send routing information very frequently, thus causing congestion or very rarely, thus preventing nodes to gain new information about the changed topology of the network. In the worst case the adversary is able to change routing protocol to operate arbitrarily or perhaps even in the (invalid) way the attacker wants. If the compromised nodes and the changes to the routing protocol are not detected, the consequences are severe, as from the viewpoint of the nodes the network may seem to operate normally. This kind of invalid operation of the network initiated by malicious nodes is called a *byzantine failure*.

4.3 Impersonation

Impersonation attacks form a serious security risk in all levels of ad hoc networking. If proper authentication of parties is not supported, compromised nodes may in network layer be able to e.g. join the network undetectably or send false routing information masqueraded as some other, trusted node. Within network management the attacker could gain access to the configuration system as a superuser. In service level, a malicious party could have its public key certified even without proper credentials. Thus impersonation attacks concern all critical operations in ad hoc networks. In the classroom example, however, the impersonation attack is not probable or even feasible. If a malicious student impersonates himself as the teacher's device, he may be able to access or destroy data that is stored in students' or teacher's devices or exchanged between them. The benefit of the attack is small: it will most likely be noticed very quickly and the information he can manipulate or have access to is not that crucial to make the attack worthwhile. In the other example the implications of successful impersonation is much more severe (again): a hostile node controlled by the enemy may be able to join the ad hoc network undetectably and cause permanent damage to other nodes or services. A malicious party may be able to masquerade itself as any of the friendly nodes and give false orders or status information to other nodes.

Impersonation threats are mitigated by applying strong authentication mechanisms in contexts where a party has to be able to trust the origin of data it has received or stored. Most often this means in every layer the application of digital signature or keyed fingerprints over routing messages, configuration or status information or exchanged payload data of the services in use. Digital signatures implemented with public-key cryptography are as such a problematic issue within ad hoc networks, as they require an efficient and secure key management service and relatively much computation power. Thus in many cases lighter solutions like the use of keyed hash functions or a priori negotiated and certified keys and session identifiers are needed. They do not, however, remove the demand for secure key

management or proper confidentiality protection mechanisms.

4.4 Disclosure

Any communication must be protected from eavesdropping, whenever confidential information is exchanged. Also critical data the nodes store must be protected from unauthorized access. In ad hoc networks such information can include almost anything e.g. specific status details of a node, the location of nodes, private or secret keys, passwords and -phrases and so on. Sometimes the control data is more critical information in respect of the security than the actual exchanged data. For instance the routing directives in packet headers such as the identity or location of the nodes can sometimes be more valuable than the application-level messages. This applies especially in critical military applications. For instance in the battlefield scenario the data of a "hello" packet exchanged between nodes may not be as interesting from the viewpoint of the enemy. Instead the identities of the observed nodes - compared to the previous traffic patterns of the same nodes - or the detected radio transmissions the nodes generate may be the information just the enemy needs to launch a well-targeted attack. On the contrary, in the classroom example the disclosure of exchanged or stored information is critical "only" from the viewpoint of a person's privacy.

5 Security in Ad Hoc Networking Proposals

5.1 DDM

Dynamic Destination Multicast protocol (*DDM*) is a multicast protocol that is relatively different from many other multicast-based ad hoc protocols. In DDM the group membership is not restricted in a distributed manner, as only the sender of the data is given the authority to control to which the information is really delivered. In this way the DDM nodes are aware of the membership of groups of nodes by inspecting the protocol headers. The DDM approach also prevents outsider nodes from joining the groups arbitrarily. This is not supported in many other protocols directly; if the group membership and the distribution of source data have to be restricted, external means such as the distribution of keys have to be applied.

DDM has two modes of operation: the *stateless mode* and the *soft-state mode*. In the stateless mode the maintenance of multicast associations and restriction of group membership are handled totally by encoding the forwarding information in a special header of the data packets; the nodes do not have to store state information. This kind of reactive approach thus guarantees that there are no vainless exchange of control data during idle periods. Thus in small ad hoc networks that need not scale up substantially, this kind of ultra-reactive approach can be extremely useful. The soft-state mode, on the other hand, requires that the nodes remember the next hops of every destination and thus need not fill up the protocol headers with every destination. In both modes the nodes must always be able to keep track of the membership of the groups. According to the authors, DDM is best suited for dynamic networks having small multicast groups. Currently the DDM draft ([8]) does not, however, propose any solutions for securing the DDM networks as such. Moreover, it does not provide any suggestions for a concrete protocol that handles the necessary

access control needed in the restriction of group membership.

5.2 OLSR

Optimized Link State Routing protocol (*OLSR*), as defined in [7], is a proactive and table-driven protocol that applies a multi-tiered approach with *multi-point relays* (MPR). MPRs allow the network to apply scoped flooding, instead of full node-to-node flooding, with which the amount of exchanged control data can substantially be minimized. This is achieved by propagating the link state information about only the chosen MPR nodes. Since the MPR approach is most suitable for large and dense ad hoc networks, in which the traffic is random and sporadic, also the OLSR protocol as such works best in these kind of environments. The MPRs are chosen so that only nodes with one-hop symmetric (bi-directional) link to another node can provide the services. Thus in very dynamic networks where there exists constantly a substantial amount of uni-directional links this approach may not work properly. OLSR works in a totally distributed manner, e.g. the MPR approach does not require the use of centralized resources. The OLSR protocol specification does not include any actual suggestions for the preferred security architecture to be applied with the protocol. The protocol is, however, adaptable to protocols such as the *Internet MANET Encapsulation Protocol* (*IMEP*), as it has been designed to work totally independently of other protocols.

5.3 ODMRP

On-Demand Multicast Routing Protocol (*ODMRP*) is a mesh-based multicast routing protocol for ad hoc networks, specified in [10]. It applies the *scoped flooding* approach, in which a subset of nodes - a *forwarding group* - may forward packets. The membership in the forwarding groups are built and maintained dynamically on-demand. The protocol does not apply source routing. ODMRP is best suited for MANETs where the topology of the network changes rapidly and resources are constrained. ODMRP assumes bi-directional links, which somewhat restricts the potential area of application for this proposal; ODMRP may not be suitable for use in dynamic networks in which nodes may move rapidly and unpredictably and have varying radio transmission power. Currently ODMRP does not define or apply any security means as such, "the work is in progress". The forwarding group membership is controlled with the protocol itself, though.

5.4 AODV and MAODV

Ad Hoc On-Demand Distance-Vector routing protocol (*AODV*), defined in [15], is an unicast-based reactive routing protocol for mobile nodes in ad hoc networks. It enables multi-hop routing and the nodes in the network maintain the topology dynamically only when there is traffic. Currently AODV does not define any security mechanisms whatsoever. The authors identify the necessity of having proper confidentiality and authentication services within the routing, but suggest no solutions for them. The IPSec is, however, mentioned as one possible solution. *Multicast Ad Hoc On-Demand Distance-Vector* routing protocol (*MAODV*), specified in [16], extends the AODV protocol with multicast features.

The security aspects currently noted in the design of MAODV are similar to the AODV protocol.

5.5 TBRPF

Topology Broadcast based on Reverse-Path Forwarding (*TBRPF*), as defined in [2], is a pure proactive, link-state routing protocol for the ad hoc networks that can also be applied as the proactive part in hybrid solutions. Each of the nodes of the network in TBRPF carry state information of each link of the network, but the information propagation is optimized by applying *reverse-path forwarding* instead of the costly full flooding or broadcast techniques. TBRPF operates over IPv4 in ad hoc networks and can also be applied within hierarchical network architecture. The authors of the proposal, however, do not suggest any specific mechanisms for securing the protocol. Finally, the protocol, just as every other ad hoc network routing protocol, can be protected with IPSec, but this approach is not currently officially in use within TBRPF.

6 Discussion

According to Zhou and Haas [19], the MANET routing protocols can seemingly tolerate the rapid changes to the topology and conditions of the networks. None of these protocols, however, seems to currently note all of the necessary security aspects adequately. Partially this is most likely due to their ongoing development. Still some drafts currently ignore the security issues by stating that the required security means are to be determined later. In this case one can get the impression that the security mechanisms will later be retrofitted to the routing protocol after the protocol itself has been tested to be robust enough. The retrofitting of the security mechanisms might, however, leave unpredictable and undetectable vulnerabilities in the system, if the protection mechanisms are not designed concurrently with the basic protocol. Moreover, some of the discussed MANET protocols have ignored the security issues completely.

The common concerns in ad hoc networks include the access control: there needs to exist a method for restricting the access of foreign nodes to the network, which requires the use of a proper authentication mechanism. Moreover, the communication between the insider nodes in the network must be protected from attacks on confidentiality. This is especially important in military applications, as was discussed. If the link-layer does not support a valid encryption scheme, such mechanism must be involved in the network layer also. The group membership is noted in all of the mentioned multicast protocols, but they do not suggest any specific access control or authorization policy protocols.

In ad hoc networks the possibility of denial of service attacks must also be mitigated, to ensure full availability in the network. In ad hoc networks malicious nodes may offer a non-existing multi-hop service to redirect traffic incorrectly and cause congestion if the node is allowed to access the network. As discussed e.g. in [6], denial of service attacks basically threaten the operation in all types of networks and they are typically impossible to prevent as such. With the use of redundancies, as described in [19], the advantages of such attacks can be significantly decreased. In addition, the distribution of responsibility and

trust from the viewpoint of the service provisioning significantly reduces the vulnerabilities that would exist in the network if centralized approaches were in use. In commercial solutions the availability of services are an especially important issue, as the network may need to scale rapidly and the credibility of the service provider is highly dependent on the operability of the network and its services.

All security mechanisms applied in networking more or less require the use of cryptography, which on the other hand implicates a strong demand for secure and efficient key management mechanism. In ad hoc networks the role of a dependable key management service is especially emphasized, given the constrained resources and possibly rapidly varying conditions in which the nodes operate. Traditional and centralized approaches cannot often be applied in the environments in which ad hoc networks operate, which forces the use of distributed services that do not rely on single resources with respect to other nodes or communication paths. This kind of approach is defined e.g. in [19].

In all the discussed MANET proposals IP forms the basis for the protocols. Thus in a few protocol proposals such as TBRPF IPSec is assumed to be able to provide a good enough privacy and authentication protection mechanism so that these issues would not need to be handled by the protocol itself. This approach has been criticized, since it produces additional (possibly manual) configuration overhead and is more or less another form of retrofitting security implementations to existing architectures.

Considering all the discussed aspects, they give a clarified picture of how important the protection of the ad hoc networking is. In addition, it is clear that the security aspects related to ad hoc networks form a very complex problem fields, given the dynamic and unpredictable nature of most ad hoc networks. On the other hand, ad hoc networks vary from each other greatly from the viewpoint of the area of application. Some ad hoc networks may not need security solutions other than simple encryption and username-password authentication scheme, as in the classroom example, while networks operating in highly dynamic and hostile environment such as in the battlefield scenario demand for extremely efficient and strong mechanisms. As the security requirements and their implications vary, a general security architecture for ad hoc network can not be constructed. The development of secure ad hoc networking framework seems to be just starting, as all the most severe security problems are not even fully solved in ad hoc networking proposals.

7 Acknowledgements

For comments and advice the author wishes to thank his tutor Catharina Candolin, Dr. Helger Lipmaa and administrative assistant Heidi Pehu-Lehtonen.

References

[1] Anon. An Introduction to Role-Based Access Control. NIST ITL Bulletins, National Institute of Standards and Technology, December 1995. [referred 7.11.2000] <http://csrc.ncsl.nist.gov/nistbul/csl95-12.txt> [in ASCII format]

[2] Bellur, B. et al. Topology Broadcast Based on Reverse-Path Forwarding (TBRPF). IETF draft, 11 July 2000. [referred 25.9.2000] <http://www.ietf.org/internet-drafts/draft-ietf-manet-tbrpf-00.txt> [in ASCII format]

[3] Corson, S. and Macker, J. Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501, January 1999, Internet Society. [referred 25.9.2000] <ftp://ftp.funet.fi/pub/standards/RFC/rfc2501.txt> [in ASCII format]

[4] Ferraiolo, D. and Kuhn, R. Role-Based Access Controls. National Institute of Standards and Technology. [referred 7.11.2000] <http://hissa.ncsl.nist.gov/rbac/paper/node2.html> [in HTML format]

[5] Haas, Z. and Tabrizi, S. On Some Challenges and Design Choices in Ad Hoc Communications. 1998. [referred 25.9.2000] <http://www.cis.udel.edu/~cshen/859_spring00/paper/milcom98.ps.gz> [in PostScript format]

[6] Hubaux et al. Towards Mobile Ad Hoc WANs: Terminodes. Swiss Federal Institute of Technology, Lausanne, 2000. [referred 25.9.2000] <http://www.terminodes.org/publications/momuc99_abstract.html> [in HTML format]

[7] Jacquet, P. et al. Optimized Link-State Routing Protocol (OLSR). IETF draft, 18 July 2000. [referred 25.9.2000] <http://www.ietf.org/internet-drafts/draft-ietf-manet-olsr-02.txt> [in ASCII format]

[8] Ji, L. and Corson, M. S. Differential Destination Multicast Specification (DDM). IETF draft, 12 July 2000. [referred 25.9.2000] <http://www.ietf.org/internet-drafts/draft-ietf-manet-ddm-00.txt> [in ASCII format]

[9] Kärpijoki, V. Signalling and Routing Security in Mobile Ad Hoc Networks. *Proceedings of the Helsinki University of Technology, Seminar on Internetworking - Ad Hoc Networks*, Spring 2000. [referred 25.4.2000] <http://www.hut.fi/~vkarpijo/iwork00/index.html> [in HTML format]

[10] Lee, S.-J. et al. On-Demand Multicast Routing Protocol (ODMRP). IETF draft, January 2000 (expired). [referred 25.9.2000] <http://www.ietf.org/internet-drafts/draft-ietf-manet-odmrp-02.txt> [in ASCII format]

[11] Moy, J. Security Architecture for the Internet Protocol. RFC 2401, November 1998, Internet Society. [referred 25.9.2000] <ftp://ftp.funet.fi/pub/standards/RFC/rfc2401.txt> [in ASCII format]

[12] Mäki, S. Security Fundamentals in Ad Hoc Networking. *Proceedings of the Helsinki University of Technology, Seminar on Internetworking - Ad Hoc Networks*, Spring 2000. [referred 25.4.2000] <http://www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/security_fund/internetworking.html> [in HTML format]

[13] Perkins, C. Mobile Ad Hoc Networking Terminology Internet draft (expired), IETF, 1998. [referred 25.9.2000] <http://www.ctron.com/support/internet/Internet-Drafts/draft-ietf-manet-term-01.txt> [in ASCII format]

[14] Perkins, C. Mobile networking in the Internet. Mobile Networks and Applications 3, 1998, p. 319-334. [referred 25.9.2000] <http://www.baltzer.nl/monet/articlesfree/1998/3-4/mnt071.pdf> [in PDF format]

[15] Perkins, C. et al. Ad Hoc On-Demand Distance-Vector Routing (AODV). IETF draft, 14 July 2000. [referred 25.9.2000] <http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-06.txt> [in ASCII format]

[16] Perkins, C. and Royer, E. Multicast Ad Hoc On-Demand Distance-Vector Routing (MAODV). IETF draft, 11 July 2000. [referred 25.9.2000] <http://www.ietf.org/internet-drafts/draft-ietf-manet-maodv-00.txt> [in ASCII format]

[17] Royer, E. and Toh, C.-K. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. 1999. [referred 25.9.2000] <http://www.ee.surrey.ac.uk/Personal/G.Aggelou/PAPERS/Adhoc_Review.ps.gz> [in PostScript format]

[18] Wang et al. Secure Routing Protocols: Theory and Practice. North Carolina State University, 2000. [referred 25.9.2000] <http://www.cis.udel.edu/~cshen/859_spring00/paper/CCR-SecureRP2.ps.gz> [in PostScript format]

[19] Zhou, L. and Haas, Z. Securing Ad Hoc Networks. 1999. [referred 25.9.2000] <http://www.ee.cornell.edu/~haas/Publications/network99.ps> [in PostScript format]