Introduction to Ad Hoc Networking

Klaus Nieminen
Networking Laboratory
Helsinki University of Technology
Klaus.Nieminen@hut.fi

Abstract

This article introduces the ad hoc networking concept. It describes the background and basic idea of ad hoc networking. After a short introduction and history parts some ad hoc networking application examples and available commercial products are discussed. This paper concentrates on wireless, mobile ad hoc networks, and describes their main problems and technical challenges. In the end of this paper, also some proposed routing protocols are reviewed and compared.

1 Introduction

Communication has changed a lot in the recent years. Mobility has become a more important factor as people have learned to be able to make a call or to access any information source anytime and anywhere. Mobile communication devices have become cheap, fast and their processing power and other capabilities have greatly increased.

We are used to the Intemet and we want to have “the network” at our disposal all the time. This has been a significant change compared to a plain fixed telephony service that was nearly the only telecommunication service people used ten to twenty years ago. This rapid development has made it possible to build ad hoc networking devices cheap and convenient. On the other hand, new applications may also require this kind of new way of communications.

The word ad hoc derives from Latin and means “for a particular purpose” or “in a way that is not planned in advance” [1]. However, the presented dictionary definitions do not fully describe the idea of Mobile Ad Hoc Networks (MANET). To be able to define the subject more precisely, we have to first observe some features common to all ad hoc networks.

The basic idea behind ad hoc networks is that they are designed to work autonomously, without any centralised infrastructure. In practise this means that network nodes should be able to communicate with each other even if no static infrastructure, such as backbone network, base stations, centralised network management functions or Internet Service Providers (ISPs) are available. In these situations, network nodes should cover the missing functions.

Mobile ad hoc network nodes can be included to nearly anything; from battleships and fighters to consumer products, such as cars, laptops, Personal Digital Assistants (PDAs) and cellular telephones. In fact, even small sensors can contain an ad hoc communication node. Therefore, the area of possible applications is really large. Typical application examples include, e.g., conferencing application, communication on a disaster area and military communications.

It is apparent that these different applications have also different requirements on, e.g., mobility, scalability, security, latency and battery energy usage. Therefore, there are also many technical challenges that have to be solved before ad hoc networks can really become common. However, the ad hoc networking concept looks promising and in the future it can have an essential role in many application areas.

1.1 History of Ad Hoc Networking

Ad hoc networking is not a new technology, but has been developed more than 30 years by now. In past years, the research and development activities were mostly funded by U.S. government and especially by Defence Advanced Research Project Agency (DARPA). This chapter describes the history of ad hoc networking by introducing the most important projects in the area of ad hoc networking. The history is summarised in Figure 1.

The origin of ad hoc networking can be traced back as far as to the ALOHA SYSTEM project [2] that was started in 1968. The project was funded by a number of U.S. state agencies, and it got also a principle support from Advanced Research Project Agency (ARPA). The ALOHA network was build to connect Hawaii university facilities with a prototype radio-linked time-sharing network, but also in order to study computer communication using radio and satellites.

Even though the ALOHA network used fixed stations and only single hops, it built the basis of distributed channel access management and so also the basis for ad hoc networking development [3]. Based on the experience of the ALOHA network DARPA began the development of Packet Radio Network (PRNet) in 1972 [4], [5].

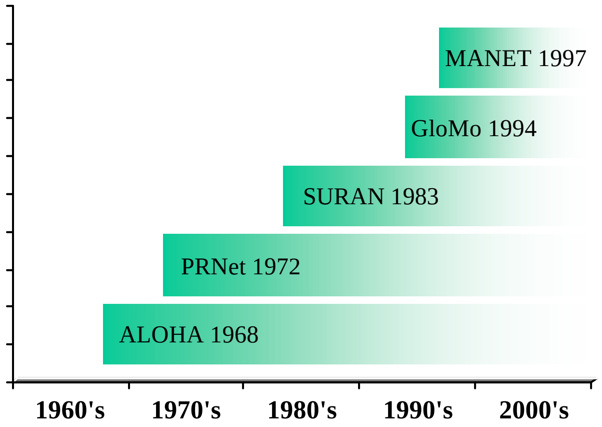

Figure 1: History of Ad Hoc Networking

The PRNet project was initiated in order to study the use of packet radio networks in a multi-hop environment. Even though PRNet used initially centralised control stations, it evolved quickly to work at distributed basis. The research done was pathbreaking, and it is worth to examine this subject a bit further.

PRNet was based on broadcast packet radios (PRs) communicating via a common radio channel. The channel sharing was dynamic, and the PRNet used a combination of the ALOHA and Carrier Sense Multiple Access (CSMA) protocols. At that time the system was rather advanced. It was half-duplex and the available data rates were 100kbit/s and 400kbit/s.

On the routing protocol side, PRNet introduced the first proactive, multi-hop routing algorithm that worked as following. Each packet radio maintains a list of its neighbouring PRs and the link quality information to them. The routes are established by packet radios that proactively announce their presence to all the other PRs. The proactive advertisements are carried out in a form of specific Packet Radio Organisation Packets (PROPs).

However, the PROP advertisements create high volume control traffic that limits the networks scalability. In fact, in PRNet the number of PRs in a network cannot exceed 138. The number of neighbouring PRs is also limited to 16. The PRNet packet radio and control devices were also seen to be too large and power hungry, and they had limited processing power.

Even though PRNet demonstrated the feasibility of ad hoc networking idea, there remained many major issues that could not yet be solved. To extend the PRNet technology further, DARPA initiated the Survivable Adaptive Networks (SURAN) project [5] in 1983. The project was designed to solve the detected problems that can be summarised to three concrete goals [5]:

- To develop a small, low-cost, low-power radio that could support more sophisticated packet radio protocols
- To demonstrate algorithms that could extend the network scalability to thousands of nodes
- To develop some techniques that would increase networks robustness and make it survivable even in the face of sophisticated electronic attack

DARPA has continued to develop ad hoc networks to satisfy military requirements. One of DARPA's latest development efforts is the Global Mobile (GloMo) project [6], initiated in 1994. The importance of different information systems is growing and from military perspective these systems should also support mobility. The GloMo project was initiated to support these future defence requirements. To be more exact, the goals of this project were to develop:

- Technology for robust end-to-end information systems in a global mobile environment
- Technology for integration of underlying commercial components into a flexible and robust multi-hop, high-bandwidth system

1.2 Current Deployment

As it can be seen from the previous section, the development of ad hoc networks has a strong military background and the research activities do still continue. Even now DARPA is supporting various research projects, such as Future Combat Systems (FCS), covering the ad hoc networking issues [7].

Despite the fact that MANET has long traditions in military, the commercial ad hoc networking development and research have just recently started. For example, the forming of the Internet Engineering Task Force (IETF) MANET working group [8] in June 1997 gave a significant lift for the commercial ad hoc networking research. The role of IETF's MANET working group is especially crucial, because it is the only party that can currently ensure the ad hoc networking protocol interoperability by introducing a widely deployed networking protocol [9].

The MANET working group was formed to introduce improved routing specification standards within the current Internet protocol stack. This specification work is purposed to lead for an open, flexible and extensible architecture for the MANET technology [10]. In more detail, the working group has the following goals [10]:

- In a near term, the MANET working group is trying to standardise an intra-domain unicast routing protocol.

- MANET working group is also going to address the security issues in intended usage environments.
- In the long run MANET working group is most probably going to address also the layering more advanced services, such as multicast and QoS extensions, on top of the initial routing technology.

The IETF's MANET working group was also fuelled by other commercial initiatives, such as IEEE's Wireless LAN (WLAN) standard, 802.11. In addition to IEEE 802.11, it is worth to mention Bluetooth that is the first commercial ad hoc radio system predicted to be used on a large scale [11]. The Bluetooth technology is developed by Bluetooth Special Interest Group founded in 1998.

2 What is the Mobile Ad Hoc Networking?

By our definition, mobile ad hoc network is a network formed without any central administration. Therefore, the network nodes have to serve also as routers and hosts. The network nodes are mobile and they are able to communicate wirelessly with each other by sending and receiving data packets.

2.1 Ad Hoc Networking

The ad hoc connectivity is based on peer communication. This is an important difference compared to cellular networks using base stations and fixed infrastructure. In addition to sending data packets directly, the nodes may also need other nodes to relay the traffic, as presented in Figure 2. The described situation is also called multi-hopping.

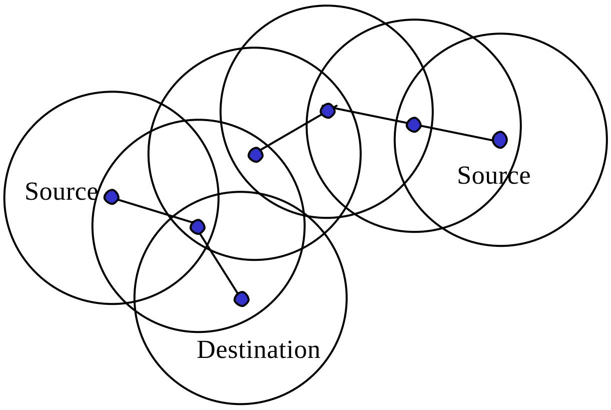

Figure 2: An example of multi-hop ad hoc communications

Because there are no separate terminals and radio units, ad hoc networks have their own network topology that is either a single-hop or a multi-hop. While single-hop network nodes send data directly from source to destination, multi-hop network nodes can use other nodes to relay their traffic.

Multiple hops increase the transmission delay, but it can be compensated with increased link rate. Therefore, the end-to-end delay may actually benefit from multiple hops [3]. In fact, multi-hopping may even be necessary to be able to reach a very distant node in available frequency range.

The large transmission range causes interference and reduces the effective bandwidth available to the network nodes by increasing the number of nodes competing for the same network bandwidth [12]. Therefore, it is beneficial to use multi-hopping or at least control the transmission range as presented in single-hop ad hoc networking example in Figure 3.

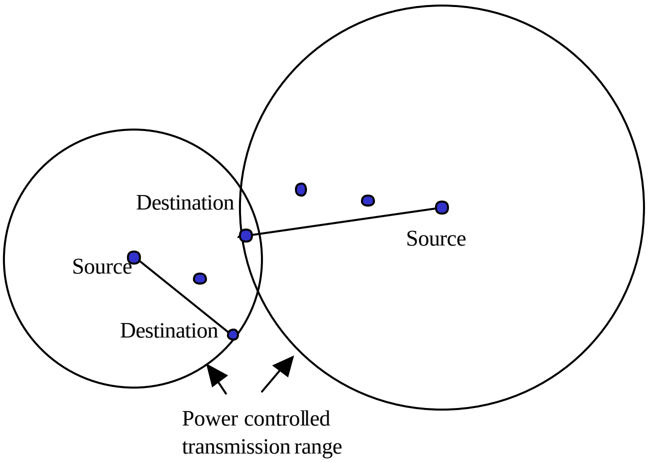

Figure 3: An example of single-hop ad hoc communications

As a summary the multi-hop networking is beneficial against single-hopping since it [3]:

- Increases the network scalability
- Reduces the interference
- Increases the overall network throughput
- Decreases the delay seen by application
- Reduces the energy consumption in data transmission

2.2 Characteristics and Requirements

From the previous definition, it is possible to derive at least the following common features and the requirements they impose. The discovered problems are discussed in more detail in Chapter 4.

- **Distributed operations**: Because a network node cannot rely on any fixed infrastructure or central administration, it is essentially distributed. Because most current systems, including telecommunication networks and a part of Internet services are centralised, the current networking functions have to be redesigned to work in the distributed environment. These functions include for example addressing and authentication.
- **Wireless connectivity**: Wireless environment causes also some problems including limited bandwidth, higher bit-error rates and fluctuation in link quality and capacity. These phenomenons are strange to the current Internet protocols, for example to Transmission Control Protocol (TCP), and therefore the protocols also have to be re-engineered to adapt the ad hoc networking environment.
- **Mobility**: The network nodes are free to move arbitrary compared to each other. This leads essentially to a dynamic network topology. The mobility will first limit the network scalability and more suitable routing protocols have to be developed. The other mobility issues are discussed further in Chapter 4.
- **Limited devices**: If we exclude different vehicles, such as cars, battle ships and fighters, from our scope, we are left with various hand-held or even smaller devices, such as sensors. These devices are limited in terms of several of their attributes including battery power and processing power. The limitations import also some requirements on protocol and application design.

As presented above, ad hoc networking covers multiple different terminals. Also the possible applications and technologies are diverse. Therefore, it is nearly impossible to define a typical mobile ad hoc network or describe a typical node. Despite of the fact that the network can vary from application to application, it is still possible to find some representative examples.

An example of ad hoc network is presented in Figure 4. The illustrated network is composed of seven network nodes, all connected wirelessly to some of their neighbours. Not only the network node capabilities, but also the used underlying transport technology can vary even within one ad hoc network. In addition to this, one node can support multiple commutation technologies.

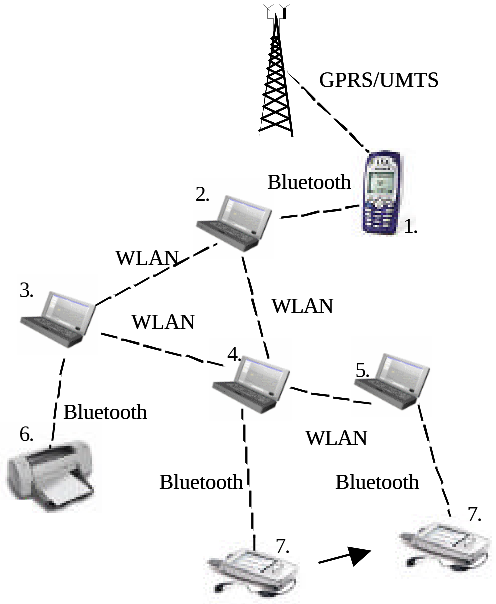

Figure 4: An example of ad hoc network

The nodes are also able to move relatively to each other breaking the existing links and forming new ones. This important ad hoc network characteristic is illustrated in Figure 4, in which node 7 moves right. The link between nodes 4 and 7 breaks and a new link between nodes 5 and 7 is established. Ad hoc networks may also contain links or gateways towards fixed infrastructure, which is presented by a cellular phone linking the ad hoc network to a cellular network.

3 Market Overview

The current market situation is discussed in this chapter. It will introduce examples from the main application areas and evaluate their requirements for ad hoc networking. This chapter also introduces the current commercial products available in the market.

As was mentioned in Chapter 1, Department of Defence (DoD) has been the main developer of ad hoc networks. Therefore, the market is still rather military oriented. However, also the commercial market is beginning to develop due to the fast technology evolution. Not only the communication products are becoming more capable, but also a new wave of data communication products and applications is emerging.

The user requirements are growing as well. People are used to cellular phones and the Internet, and they want to be able to communicate anytime and anywhere. They want to have similar, convenient services to be available, and ad hoc networking can potentially offer some new possibilities for this purpose.

Personal area networks and embedded network devices can bring the network around us to offices, shopping centres and homes. Ad hoc networking brings also totally new possibilities for machine-to-machine communication, but it can create also some "killer applications", such as extended remote control or applications that can handle some of our routines and communication needs.

Both industry and military sectors will when benefit from cheaper and more advanced solutions introduced by the mass market. In these sectors the applications are more mature, but the price has been a prohibitive cause. The ad hoc networks benefit from the corporate structure of military and industry sectors, thus it is natural to divide ad hoc applications to the following segments:

- Consumer applications
- Corporate & government applications.

Not only consumers' individual behaviour, but also the lack of suitable business models for the operators is hindering the introduction of commercial applications. In fact, even the basic idea of ad hoc networks is operator independent, and it can help people to bypass operator services, for example by offering a neighbourhood telephone service [9].

3.1 Application Examples

Ad hoc networks can be used by military, industry and consumers, and therefore the variety of possible different applications is huge. This chapter introduces some typical application examples to the reader, and discusses their role and the requirements they impose. Some of these applications can be strictly categorised to be, for example, government application, while some other applications, such as personal area networking, are equally applicable to all user groups.

3.1.1 Conferencing

The current office environment is heavily computerised and the need for collaborative computing may be even greater when the office local area network infrastructure is not available. Conferencing might be the most typical ad hoc networking application example, but it really shows us some clear benefits. The main problems are related to external system connectivity that is further discussed in Section 4.2.

An ad hoc network is more convenient than a wired Ethernet. It can also be cheaper or more secure compared to the use of possibly available cellular or Internet infrastructure. The widespread use of Bluetooth technology can also extend conferencing application to even more ad hoc manner. As an example, this could mean information transfer between accidentally met people.

3.1.2 Personal Area Networking

Today people own various portable, personal equipments, such as digital camera, laptop, MP3 player, mobile phone or PDA. Currently many of these devices are used separately, but in the future they could all interact. The idea of Personal Area Network (PAN) is to create a highly localised network that enables information to flow seamlessly between these devices. Of course in the future, these nodes can be included also to eyeglasses and belts, but the concept is also applicable to home electronics more widely.

To enable these networks, we need a cheap, short-ranged radio link technology and the strongest candidate seems to be Bluetooth [13]. Bluetooth is an industry standard that has lately received also IEEE's support. It operates in Industrial, Scientific and Medical (ISM) band at 2,4 GHz using frequency-hopping.

Bluetooth networking is based on star-shaped piconets including one master and maximum seven slaves. The master controls and relays traffic in a piconet. Furthermore, two or more piconets can form a scatternet extending the network size and overall capacity. In these cases one Bluetooth unit can be a slave member of multiple piconets, but master in just one.

The idea of Bluetooth fits very well to ad hoc networking and Bluetooth could have real possibilities to push ad hoc networking to mass market. However, piconet and scatternet formations are problematic in terms of long formation times and un-ideal configurations. Therefore, there are still many issues, from physical to network layers, to be solved.

3.1.3 Emergency Services

From emergency services' point of view, the ability to establish communication even without any fixed infrastructure is vital. Of course, normally, when this really widely covered infrastructure is available, ad hoc networking provides nothing new. But, what about if the existing infrastructure is damaged, out of service or there is no coverage for other reasons?

Ad hoc networks can help to overcome these shortcomings, for example, during disasters, terror strikes or natural catastrophes. It is also good to realise that service failures are much more common due to dead spots, e.g., in sea or underground or during a power loss.

Ad hoc networking could enable the police, firemen and other critical emergency staff to work in these situations, but it also imposes some severe threats, like security treats. Also the lack of centralised administration may cause some difficulties. The strengths are still much larger, especially because the importance of network applications and services is increasingly growing.

3.1.4 Sensor Dust

Microcomputers' computational capacity and memory storage have significantly increased, which has enabled smaller and more powerful wireless devices to be developed. The recent advances in hardware technology and engineering design have also reduced cost, power consumption and size of wireless devices and micro electromechanical systems [14].

This development has made it possible to design autonomous, compact, low cost, mobile nodes that contain one or more tiny sensors, computational and communication capabilities and a power supply [14]. These "dust nodes" could fit into only a few cubic millimetres, so they could become small enough to remain in the air for hours or even days.

This technology would be really useful for many different user groups, such as:

- Emergency staff could use these sensors to detect possible hazardous chemicals or gas.
- Military could use ad hoc devices for similar purposes to detect, e.g., war gas or to do intelligence operations. In both previous cases the sensors could be dropped from a plane to network and gather the required information.
- Industry could also use these sensors to control their processes or to find malfunctions.

In many cases the battery life-time may also be the life-time of the whole sensor. Therefore, these sensor dust applications are very challenging products imposing strict power consumption requirements on ad hoc data transmission and routing protocols.

3.2 Commercial Products

Even though it is possible to identify a large variety of ad hoc networking applications, it is much harder to find any existing commercial products. The main reason for this is that there are still rather few commercial products available. Another reason is that the commercial products are not typically marketed as ad hoc products. Some other common names that can reveal the use of ad hoc networks are, for example, peer communications, mesh networking and ubiquitous communications.

Even though the consumer segment looks most promising in the future, there are nearly none commercial products currently available. The main reasons behind this are the problems encountered with Bluetooth and IEEE 802.11 technologies. The current Bluetooth chips and IEEE 802.11-based PC cards support only ad hoc connectivity and therefore, they can hardly be considered as real ad hoc networking products. Some military systems and other tactical products including emergency, exploration and communication applications may use ad hoc networking, but the publicly available information is nearly non-existent. In fact, also in the industry segment the ad hoc networking is well hidden behind embedded and complex integrated systems.

Even though the range of commercial products is small and the available information is meagre, there are some ad hoc networking products in the market. In addition to complex integrated products, they include also some applications, like peer-to-peer network clients, Bluetooth and IEEE 802.11 network simulators and software that enables multi-hop connectivity.

4 Problems in Ad Hoc Networking

As many people have forecasted, the ad hoc networks can answer many of our future communications needs. According to William Webb [15], wireless, short-range communication devices will be embedded to many of our items and nearly everyone is going to carry a wireless communicator. This offers great possibilities and especially challenges for ad hoc networking, because there still are rather many problems to be solved.

This chapter discusses some of the main problems, but does not try to propose detailed solutions. The purpose of this chapter is to introduce reader with the main problems, technology limitations and future research possibilities.

4.1 Consumer Applications

Ad hoc networks have potentiality in consumer market, but there are a lot of difficulties that have to be solved before these possibilities can be realised. Consumer applications are touched by the same difficulties as other applications using ad hoc networking, but they have also some problems of their own.

Spotting of "free riders" that only use the network, but do not relay others traffic is hard [9]. Therefore, especially consumers should be motivated to co-operate. Today, no proper solution exists, but if electrical cash will become more common, it can be the solution.

Ad hoc network coverage is currently non-existent and even after a mass-market launch it will be spotty. This is a real chicken-egg problem, because with a low node density, no network can be formed at all. Of course the development can start from PANs that do not essentially require a contact with a larger network, but the question is still valid.

4.2 External System Connectivity

Many applications need a connection to some external systems, especially to the Internet. This is, of course, advantageous from a network's perspective, but very exhausting from edge node's point of view, especially if we are talking about power scarce hand held devices. For further information see Sections 4.1 Consumer Applications and 4.5 Scarce Battery Power.

As was said, it is advantageous to establish Internet connectivity. The edge node willing to offer Internet connectivity can, for example, advertise itself as a default router. This "edge node" can also provide full service mobility by mobile IP, if it works as a foreign agent [3]. However, it is highly uncertain that Internet connectivity could be provided to an arbitrary ad hoc node. Therefore, also availability of the typical Internet services, central authorities and management functions is questionable.

4.3 Limited bandwidth

Compared to fixed connections, the wireless bandwidth is a scarce resource. In addition to lower available data transmission rate, this causes problems in designing routing protocols, because the bandwidth has to be preserved for actual data transmission as much as possible. Considering different routing protocols, the available bandwidth limits also network scalability, because the bigger the network is, the more and larger routing updates have to be sent.

Combined with scarce battery power, limited bandwidth may also increase the temptation to delay or even drop other users' traffic in public networks to be able to transmit own packets. This may be especially dangerous in bottleneck nodes.

4.4 Scalability

The dynamic network topology and the possible lack of aggregation possibilities lead to direct scalability problems [9]. The loss of aggregation leads to bigger routing tables. Node's mobility is even a bigger problem, because the routing information changes when the node moves, and to maintain routing tables, we have to send control messages around the network.
When the nodes move quickly related to each other, also more control messages has to be sent. The increasing number of control messages reduces the available bandwidth, which places one constrain for network scalability. The amount of sent control messages depends on the used algorithm, but it can also impose some other problems like long convergence times or too big latency.

Therefore, the network scalability is not only affected by the node mobility, but also by the latency requirements placed by the used applications as presented in Chapter 5 Ad Hoc Routing . As a conclusion, the network is scalable as long as these bandwidth, convergence and latency issues are in manageable extend [9].

4.5 Scarce Battery Power

The most ad hoc networking devices are small, handheld equipments with only scarce battery power resources. For example, in sensor applications, discussed in Section 3.1.4 Sensor Dust, battery can even define the lifetime of an application. Therefore, also the battery power usage is one of the key research problems that divides to routing and actual data transform parts.

First, the packet forwarding is costly in terms of power consumption. Therefore, this may limit the willingness of mobile nodes to offer themselves as immediate forwarding nodes. However, this is really essential, because without available forwarding nodes the ad hoc network does not work. In consumer applications this problem may also result the node to attempt to freeload the network, without offering any forwarding service by itself [9]. This problem is discussed further in Section 4.1 Consumer Applications.

The battery usage may be controlled by altering the transmit power. The use of smaller transmit power seems to conserve energy, even though it results multi-hopping [3]. Multi-hop networking makes routing more demanding and more power consuming operation, which is also another main power drain in ad hoc networks.

Power can also be conserved by sending routing information less frequently or just on-demand. This trade-off between frequent route updates and battery power utilisation is one of the major engineering decisions, for ad hoc routing protocols, because updates sent less often increase also latency [9]. Also other techniques are developed to control the power usage, such as using a sleep mode.

4.6 Security

The mobile ad hoc networks have many features that make them especially vulnerable for security problems in all layers. They uses open medium and they have a dynamically changing topology. Also the lack of centralised infrastructure and cooperative algorithms make it impossible to apply the fixed network mechanisms to ad hoc environment. In more detail, ad hoc networking imposes three different threats [16].

- Wireless media makes ad hoc networks vulnerable for numerous attacks ranging from passive eavesdropping to active interference. The lack of clear line of defence makes it harder to defend these attacks and therefore any node has to be prepared for both direct and indirect attacks.

- Mobile ad hoc nodes are autonomous and able to roam independently. This makes them easier targets for captures. Captured nodes are harder to detect than in fixed network, and because of networks' cooperative nature the attacks can also be far more damaging. For example, by distributing false routing information, one node can eventually paralyse the entire network or even worse, it can hijack all information to be routed by it.
- The third and maybe the worst treat is imposed by the distributed decision making and the lack of centralised infrastructure and certificate authorities. This results some difficulties for both routing protocols and overall information security, because of harder and less trustworthy key and certificate distribution. Especially in large scale it is really hard to know whom to trust. Also the scalability of the solution can become a problem.

As a summary, information can be stolen or altered without end user's knowledge. The service can also be denied easily. The transmitted information is travelling trough many, possible untrustworthy nodes, and in principle an attacker has only to wait for new targets instead of actively pursuing them. Because of co-operating protocols, also the whole network is much more vulnerable, especially because the current devices lack good mechanisms to authenticate a particular user to a particular device. Also the problems of tracking certain users in this environment, makes ad hoc network more attractive targets [17].

5 Ad Hoc Routing Protocols

The numerous problems, discussed in Chapter 4 Problems in Ad Hoc Networking, make also the design of ad hoc routing protocols more challenging. The current routing protocols used in the Internet are insufficient to work well in ad hoc environment and at least some modifications have to be done [18]. The main objective for this development is that the shortest path first protocols, such as distance vector and link state protocols have a high message complexity.

Due to the limited bandwidth the message complexity should be kept low. Along with rapidly changing topology, it is very important to find routes quickly. This may require even use of sub-optimal routes. Of course the routing protocols should also be efficient, self-organised and self-configured.

Due to these problems, routing is one of the hottest and currently most researched topics in the ad hoc networking area. For example, alone in the IEEE journals in 2001, there were at least 73 articles related to ad hoc routing.

5.1 Routing algorithms

Traditionally, the routing protocols used in packet-switched networks have been based on either link-state, e.g., Open Shortest Path First (OSPF), or distance-vector, e.g., Routing Information Protocol (RIP), algorithms [9]. This division provides also a good way to categorise routing protocols according to the information they use.

In the link-state algorithms the routing table is formed from link state information. This information is gathered from all links that have been established between the other nodes in the network. However, the link-state algorithm is not very well suited to highly dynamic networks, because of the relatively large bandwidth requirement it imposes.

A distance-vector algorithm is another popular routing algorithm that is based on shortest path first algorithms. Typically it stores only information about the next hop to the desired destination. Therefore, it has only a little information about the nodes that are not directly connected to it. The name distant-vector derives from the cost metric, which is typically just a distance, stored into its routing table.

The distance-vector algorithms are easy to program and they need less memory than the link-state algorithms [9]. They also enable more localised routing updates, because all the information is not stored into every node. However, the distant-vector algorithms have also drawbacks, like very slow convergence.

In addition to these traditional algorithms, also some other algorithms have been proposed to ad hoc networks. Below there are two examples of taken different approaches.

- Link Reversal Routing (LRR) is purposed to adapt the rapid topology changes by localisation to algorithms reactions. It maintains a source tree called a directed acyclic graph (DAG) rooted at the destination, instead of distributed network state needed for shortest path first routing.
- Source Routing (SR) is a reactive routing protocol also designed to work in a dynamic, multi-hop ad hoc environment. SR is based on obtaining the source information from received packets. Every packet carries an ordered list about the nodes it has passed in its header.

5.2 Proactive Versus Reactive Protocols

Maybe the most interesting classifying feature of ad hoc routing protocols is the way they obtain the routing information:

- Do they keep track of all possible routes, even if there is no need to do that? This approach is called proactive or table-driven approach.
- Do they track the destination, only when it is required? This approach is called reactive or on-demand approach.

The proactive protocols keep track of routes for all destinations. The main benefit of this approach is that it imposes a minimum initial delay when starting communication with an arbitrary destination. However, it suffers from additional control traffic that is caused by continuous updates of stale route entries. This can cause scarce bandwidth resources to be wasted on fixing unused routes. Extra control packets may also create further congestion by reserving scarce queuing space [9]. Due to the higher priority of control packets, normal data packets will be lost, resulting to retransmissions and even further congestion.

Table 1: Overall comparison between reactive and proactive routing protocols [19]

Compared feature	On-demand, reactive	Table-driven, proactive
Availability of routing information	Available when needed	Always available regardless of need
Routing philosophy	Flat	Mostly flat, except CGSR
Periodic updates	Not required	Required
Coping with mobility	Use localised route discovery as in ASB and SSR	Inform other nodes to achieve a consistent routing table
Signalling traffic generation	Grows with increasing mobility of active routes	Greater than that of on-demand routing
Quality of service support	Few can support QoS, although most support shortest path	Mainly shortest path as the QoS metric

Thus, proactive routing protocols do not fit well in highly mobile environment, but are reactive protocols then better? Reactive protocols have been designed to function in more dynamic environment. They discover and maintain routes on an as needed basis. Therefore, maintaining the routing tables use less bandwidth, but at a cost of increased latency. The proactive and reactive protocols are compared in Table 1.

It has also been proposed to keep track of multiple routes between source and destination nodes. This “multipath routing” may help to discard stale routes, even if they are not in active use [9].

5.3 Proposed Routing Protocols

As was said in the beginning of this chapter, routing seems to be currently the most studied topic in ad hoc networking area. Thus, a number of routing protocols have been proposed, but their comparative performance is not well understood [18].

The scalability of the different routing protocols has only been studied in rather small networks, because the large simulations take too much time and memory [9]. It is safe to say that the ad hoc network cannot scale to a size of the Internet, but the more concrete upper limit for different protocols is still unclear. However, even typical simulations done with 50 to 100 nodes shows the poor performance of current protocols.

Thus, there are multiple approaches that can be used to categorise routing protocols. For example, it could be considered whether a flat or hierarchical addressing scheme should be used [19] or if the protocol is capable for multicast routing. Anyway, this paper is meant to give only a short introduction to ad hoc networking. Therefore, only a simple classification is used here. Table 2 shows some proposed routing protocols classifying them to reactive or proactive categories.

Table 2: Comparison of some routing protocols

Routing protocol	Way of obtaining routing information
ABR	Reactive
AODV	Reactive
CBGR	Proactive
CBRP	Reactive
DSDV	Proactive
DSR	Reactive
FSR	Proactive
OLSR	Proactive
SSR	Reactive
STAR	Proactive
TORA	Reactive
WRP	Proactive
ZRP	Proactive & reactive

For more information on listed routing protocols, see Perkins, Ad Hoc Networking [9].

Acronyms

ABR: Associativity-Based Routing
AODV: Ad Hoc On -demand Distant-Vector
ARPA: Advanced Research Project Agency
CBGR: Cluster Based Gateway Switch Routing
CBRP: Cluster Based Routing Protocol
CSMA: Carrier Sense Multiple Access
DARPA: Defence Advanced Research Project Agency
DSDV: Destination Sequence Distant-Vector
DSR: Dynamic Source Routing
FSR: Fisheye State Routing Protocol
GloMo: Global Mobile
IEEE: Institute of Electrical and Electronics Engineering
IETF: Internet Engineering Task Force
ISM: Industrial, Scientific and Medical
ISP: Internet service provider
MANET: Mobile Ad Hoc Network
OLSR: Optimised Link State Routing Protocol
OSPF: Open Shortest Path First
PAN: Personal Area Network
PDA: personal digital assistant
PROP: Packet Radio Organisation Packets
RIP: Routing Information Protocol
SSR: Signalling Stability based adaptive Routing
STAR: Source Tree Adaptive Routing
SURAN: Survivable Adaptive Networks
TCP: Transmission Control Protocol
TORA: Temporally-Ordered Routing Algorithm
WLAN: Wireless Local Area Network
WRP: Wireless Routing Protocol
ZRP: Zone Routing Protocol

References

[1] Oxford Advanced Learner's Dictionary, Oxford University Press, 1989, ISBN 0194311104

[2] Kuo, THE ALOHA SYSTEM, ACM SIGCOMM Computer Communication Review volume 25 number 1, January 1995, ISSN # 0146-4833

[3] Frodigh, Johansson and Larsson, Wireless ad hoc networking – The art of networking without a network, Ericsson Review No. 4, 2000

[4] Jubin and Tornow, The DARPA Packet Radio Network Protocols, Proceedings of the IEEE Special Issue on Packet Radio Networks, January 1987

[5] Freebersyner and Leiner, A DoD Perspective on Mobile Ad Hoc Networks, In C.E. Perkins (editor), Ad Hoc Networking, Addison Wesley, December 2000

[6] Leiner, Ruth and Sastry, Goals and Challenges of the DARPA GloMo Program, IEEE Personal Communications, December 1996

[7] Defence Advanced Research Project Agency's www-homepages, http://www.darpa.mil/

[8] Internet Engineering Task Force, MANET working group charter, http://www.ietf.org/html.charters/manet-charter.html

[9] Perkins, Ad Hoc Networking, Addison Wesley, December 2000

[10] Macker and Corson, Mobile Ad Hoc Networking and the IETF, ACM Mobile Computing and Communications Review, vol 2, number 1, January 1998

[11] Haartsen, The Bluetooth Radio System, IEEE Personal Communication, February 2000

[12] Royer, Perkins, Transmission Range Effects on AODV Multicast Communications, To appear in ACM Mobile Networks and Applications special issue in Multipoint Communication in Wireless Mobile Networks, 2002

[13] Johansson, Kazantzidis, Kapoor and Gerla, Bluetooth: An Enabler for Personal Area Networking, IEEE Network, September/October 2001

[14] Kahm, Katz and Piester, Mobile Networking for "Smart Dust", In Proceeding of the Fifth ACM/IEEE International Conference on Mobile Computing and Networking, August 1999

[15] Webb, The Future of Wireless Communications, Artech House, 2001, ISBN 1-58053-248-0

[16] Zhang, Lee, Intrusion Detection in Wireless Ad-Hoc Networks, Proceedings of the sixth annual international conference on Mobile computing and networking, ACM Press 2000

[17] Ghosh and Swaminatha, Software security and privacy risks in mobile e-commerce, Communication of the ACM, February 2001

[18] Das, Castaneda and Yan, Simulation-based performance evaluation for routing protocols for mobile ad hoc networks, ACM Mobile Networks and Applications 5, 2000

[19] Royer, Toh, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, IEEE Personal Communications, April 1999