WWRF/WG4/Ad-hoc Networking -Subgroup

White Paper

Editors:
Srdjan Krco (Ericsson Systems Expertise)
Bernard Hunt(Philips)
Frank Fitzek (acticom)

Contributors:
Frank Fitzek (acticom)
Halim Yanikomeroglu (Carleton University)
David Falconer (Carleton University)
Seshaiah Ponnekanti (Fujitsu)
Bassam Hashem (Nortel Networks)
Konrad Wrona (Ericsson Systems Expertise)
Wolfgang Zirwas (Siemens)
Erik Weiss (Aachen University of Technology)
Bernard Hunt (Philips)
Srdjan Krco (Ericsson Systems Expertise)

Version 1.0

17th June 2002

Abstract

Ad-hoc networks are formed by users or devices wishing to communicate, without necessity for the help or existence of any infrastructure or centralised administration. Each node has a wireless access interface (Bluetooth, WLAN, HiperLAN2, UWB, etc.) and is free to enter or leave the network at any time. Due to the limited range of a node's wireless interface, multiple hops may be needed for communication. Ad-hoc networks can function as standalone networks meeting direct communication needs of their users, or as an addition to infrastructure based networks to extend or enhance their coverage.

Ad-hoc communication becomes a viable solution especially in situations of missing or incomplete network. Applications of ad-hoc communication include sensor networks, commercial and educational use, emergency cases and military communication.

Ad-hoc networks have attracted a lot of attention in the research community over the last couple of years. Research issues cover many different areas and multidisciplinary expertise is required to tackle these problems. In this paper an overview of research activities and issues in this area is given. Some of the current solutions along with open issues are presented.

1. Introduction

Networks that we know today are based on pre-established relationships between a network subscriber and a network operator. If a user wants to access a mobile network, a contract with a network operator is required. If a user wants to access the Internet, a contract with an ISP is required. Even when accessing a corporate network, a predefined configuration of the client device is required.

At the same time, we are witnessing a fast proliferation of various wireless devices. Mobile phones have already become an integral part of everyday life. Laptops, PDAs, pagers, game consoles and other similar devices are following the trend. Various sensors are used in industry and there is a huge push towards enabling them with wireless access to ensure easier deployment and accessibility. With all these communication capable devices available in the environment, a need to connect them easily has arisen. Obviously, it is not possible to establish a contract with every device owner with whom we might want to communicate for many reasons. There are huge numbers of existing devices providing different services and it is impossible to know in advance which service we might need and which particular device can offer that service. Even if we could establish a relationship with required devices, manual configuration of each connection would be a very complex task. These reasons have initiated research that should provide a new communication paradigm that supports ad-hoc establishment of relationship between devices and automatic configuration of communication.

According to WWRF's "Book of Visions" and ISTAG "Visions", future networks will use ad-hoc communications extensively [1], [2]. The future *Wireless World*, as envisaged by the WWRF, will enable connectivity for "everybody and everything at any place and any moment". In the centre of the *Wireless World* is a Personal Area Network (PAN), which is an example of an ad-hoc network. Various forms of ad-hoc communications are taking place on all *Wireless World* spheres as well. PAN devices can interact with devices in the person's environment, or are can access an infrastructure-based network using multi-hop routes via other nodes in an ad-hoc network.

Some other examples of ad-hoc networks, beside PANs, are body area networks, networks of sensors and actuators, home networks, vehicular networks and very high data rate hotspots. These networks could be used in many scenarios ranging from small office environment to large-scale sensor networks:

- Sensor networks - for communication between intelligent sensors;
- Commercial use - for setting up communication in exhibitions, conferences, or sales presentations;
- Personal use - for non-commercial transfer of data between devices or persons;
- Search and rescue operations - for communication in areas without adequate wireless coverage or when the existing communication infrastructure is non-operational due to a natural disaster or a global war;
- Military applications for fast establishment of communication during the deployment of forces in unknown and hostile terrain.

2. Ad-hoc Networks Characteristics

In general case, ad-hoc networks could be defined as networks formed by users or devices wishing to communicate, without the necessity for the help or existence of any infrastructure or previously established relationship between the potential network members. Nodes in ad-hoc networks can be very diverse in terms of various characteristics like throughput, transmission power, energy

resources, size or cost. Each node has a wireless access interface (Bluetooth, WLAN, HiperLAN2, UWB, Infra-Red, etc.) and is free to enter or leave the network at any time. Ad-hoc networks can function as standalone networks meeting direct communication needs of their users, or as an addition to infrastructure based networks to extend or enhance their coverage. Due to the limited range of a node's wireless interface, multiple hops may be needed for communication. Nodes are running routing algorithms to establish routes in the network and are forwarding packets destined for other nodes.
Ad-hoc communication, obviously can take place in various scenarios. Depending on the scenario, different issues can be encountered. In PANs, device and service discovery and network configuration are critical challenges. In larger networks, where multi-hop communication is required, routing becomes very important. If the access to a cellular network or Internet is required, addressing, authorization and charging have to be solved. Security is an issue regardless of scenario, mainly due to the fact that unknown nodes relay traffic. Bluetooth, WLAN, UWB or some other wireless access technology could be used for data transmission. Specific features of each technology have an impact on possible solutions (for example, UWB provides good location estimation and that information could be used in routing protocols).
In the following paragraphs these research issues are described and current solutions presented.

3. Application Scenarios

Ad-hoc networks could be useful in many scenarios. The first requirements for these networks stem from the military applications. On a battlefield, an ad-hoc network among soldiers could be established so that their position and health condition can be constantly monitored. Various sensors could be deployed to track movement of the enemy forces or to monitor ammunition stock.
Beside military applications, various other scenarios are envisaged that could utilize capabilities of ad-hoc networks. In office environment ad-hoc communication between participants of a meeting can be established for data exchange. After a catastrophe, vital communication links could be established using the principles of ad-hoc networks. Environmental pollution can be monitored using large sensor network that organizes automatically and sends data to a centre using multi hop routes.
Communication in a personal area network is established opportunistically, depending on the person's needs and the immediate environment.
Large, pure ad-hoc networks are still far from deployment due to various technological and human limitations (how to stimulate someone to forward packets for other network participants, how to protect a network from those trying to cheat and so on). It is envisaged that ad-hoc communication will mainly be used as an extension of infrastructure-based networks or in a personal bubble. Utilization of ad-hoc communication principles is suggested for enhancements of infrastructure networks as well.
The following paragraphs describe some of these scenarios.

3.1. Interoperability with fixed/overlay networks

The combination of ad-hoc networks with fixed/overlay networks is very attractive, because it allows usage of a wider range of services. This can be primarily achieved by connecting one node that is linked within the ad-hoc network directly to the fixed network. The link to the fixed network can also be established by another wireless connection with another node that has an existing link to the fixed network. Nodes that support the transition from the ad-hoc network to an overlay network are acting as routers. Nodes trying to use services from the overlay network have to detect such a border router. Authentication of the nodes can be done in two ways:

- The border routers take responsibility for all the underlying ad-hoc nodes, or
- The traffic of the ad-hoc nodes are tunneled to an authentication server in the overlay network, which is doing the authentication process.

An example of ad-hoc networks combined with fixed and overlaying networks is given in Figure 1. Wireless nodes are distributed over a given area. Some of the nodes connect directly to a wired access point. Because of the missing infrastructure, not every access point can be connected hard-wired. Therefore virtual access points are introduced. Virtual access points are connected directly or over multi-hop with the wired access points. Wireless nodes can connect to any of the access points in dependency of their location/signal strength. In case nodes cannot connect to any access point (like the nodes between buildings b) and c) they will use other nodes as routers for multi-hopping based access to the access points.

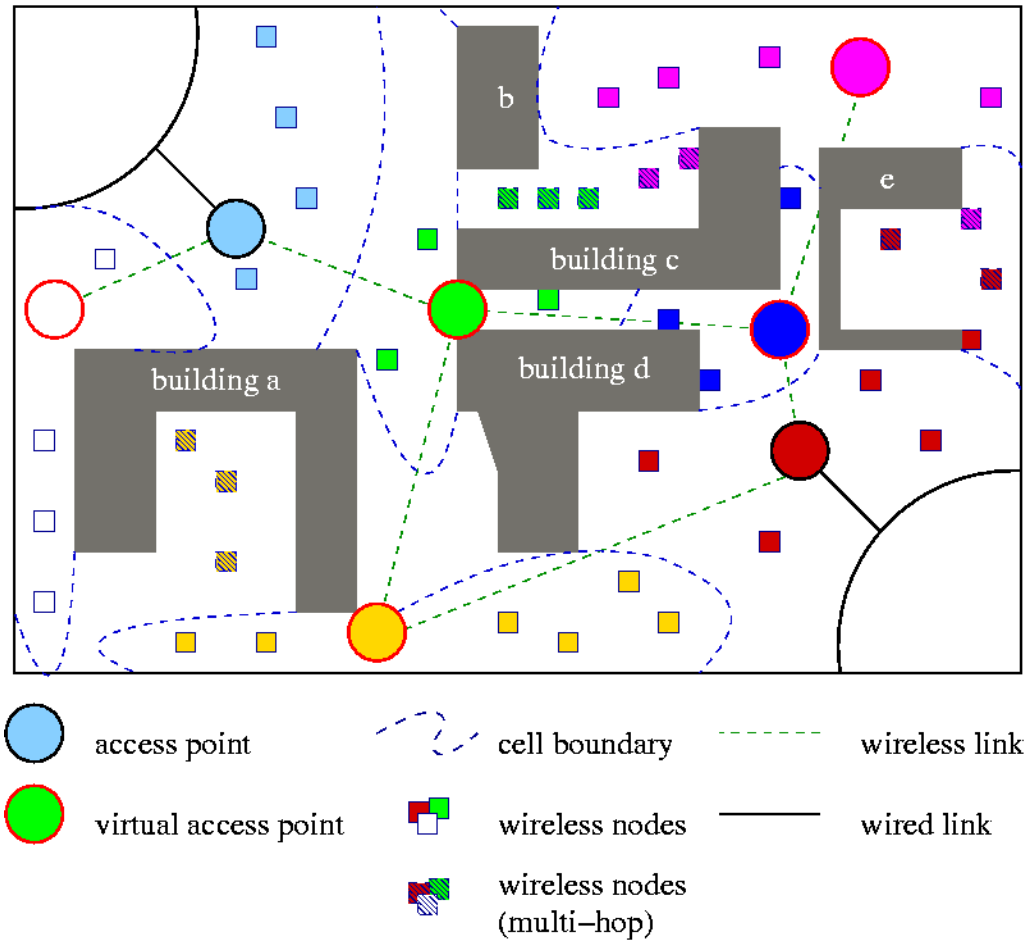

Figure 1 An example of a combination of ad-hoc networks with fixed and overlaying networks

As it is stated above, ad-hoc networks may serve as an extension of fixed networks as well. There are many issues connected with this scenario. Some questions are still open such as:

- How is authentication performed and who is authenticated – gateway node or user's node?
- Is the gateway node acting as a bridge or as a router?
- How is the mobility of ad-hoc networks supported, i.e. is it possible for an ad-hoc network to change its point of access to the fixed network without interrupting current communication or for an individual node to transfer between ad-hoc networks without losing the connection to the fixed network?

3.2. Multi-hop-Augmented Infrastructure-Based Networks

Simple calculations indicate that the provision of the very high data rates envisioned in future wireless systems in reasonably large areas (i.e., beyond small disconnected pockets) does not seem to be feasible unless significant new spectrum is released or the density of the access points is increased dramatically. Currently, there is no indication that significant new spectrum will be available in the near future; and, a drastic increase in the number of access points is not economically justifiable.

In recent years, there have been significant advances in signal processing techniques (such as interference cancellation algorithms) and collocated antenna architectures which are generally referred to as smart antennas (such as MIMO and adaptive antennas). Although incorporation of these techniques in future wireless systems is crucial, for practical reasons, these techniques alone do not seem to be sufficient in enabling almost-ubiquitous very high data rate coverage. For instance, it may be infeasible to deploy complex antenna systems at wireless terminals; besides, in the presence of heavy shadowing, even the smartest antennas will not be of much help.

Therefore, more fundamental enhancements are necessary for the very ambitious capacity, throughput, and coverage requirements of future. Towards that end, in addition to advanced signal processing techniques, some major modifications in the wireless network architecture itself, which will enable effective distribution and collection of signals to and from wireless users, is sought. The integration of multihop capability in conventional wireless networks is one such promising architectural upgrade.

Towards that end, in the last few years there has been quite an interest in the generic multihop networks in both industry and academia, such as the "seed" concept in 3GPP, coverage extension of HiperLAN2 through relayers, user-cooperative diversity, LMDS/MMDS mesh networks. The intermediate relayers/routers in such multihop-augmented networks may be some fixed low-complexity entities (like "seeds" in the cellular multihop case [3GPP terminology]), or the other wireless terminals in the network (although routing through wireless terminals is not practical in the FDD mode unless non-trivial hardware changes/updates are made). Advanced antenna technologies can (and should) also be incorporated in these networks to increase the effectiveness in signal delivery further.

It is worth emphasizing the basic difference in the fundamental goal of the conventional ad-hoc and the described multihop-augmented infrastructure-based networks: while the defining goal of the ad-hoc networks is the ability to function without any infrastructure, that goal in the latter types is the almost-ubiquitous provision of very high data rate coverage and throughput.

There are many issues to be investigated towards a successful integration of the multihop capability in conventional wireless networks. For instance, the advantages and disadvantages of using fixed versus mobile relayers (routers), and of performing relaying in analog (amplify-and-forward) versus digital (decode-and-forward) form, have to be investigated. Other pertinent issues within the context of multihop-augmented networks include the load balancing capability (by diverting the traffic with relayers as necessary), signaling overhead, relaying interference, possible cap on the number of hops, incurred latency and its impact on QoS, relayer complexity and functionality, scheduling, radio resource management, and novel diversity techniques.

3.3. Virtual Personal Distributed Networks (VPDN)

The advent of Bluetooth and other similar short-range wireless systems will encourage a development of a wide variety of devices carried or used by individuals. Moore’s law predicts that processing speed and memory capacity doubles every 18months. Availability of increasing storage and processing capability within individual devices will permit applications to be distributed across the networks.

A PAN comprises devices in a person's immediate environment that join and leave the PAN depending on user's requirements. Although a PAN is limited to a short range several scenarios require presence of remote devices in the PAN. For example, parents want to establish a "family network" comprising their and their children's PANs in order to stay in constant touch regardless of location of each person. Home security system, car alarm system or another PAN could be parts of a personal network (Figure 2) enabling easy monitoring of personal property.
The extension of a PAN can be done via infrastructure networks (Internet, cellular networks), PANs belonging to other users, car networks, home networks etc. The significant challenges have to be overcome before deployments of VPDNs. VPDNs are extremely dynamic with continuously changing topology. Configuration has to be simple and performed automatically. Secure transmission of data is very important in such distributed environment where many unknown devices and networks have access to user data. A great variety of devices with different characteristics, capabilities and different wireless and network technologies will be involved and protocols have to take into account all the specifics of each device and each technology.

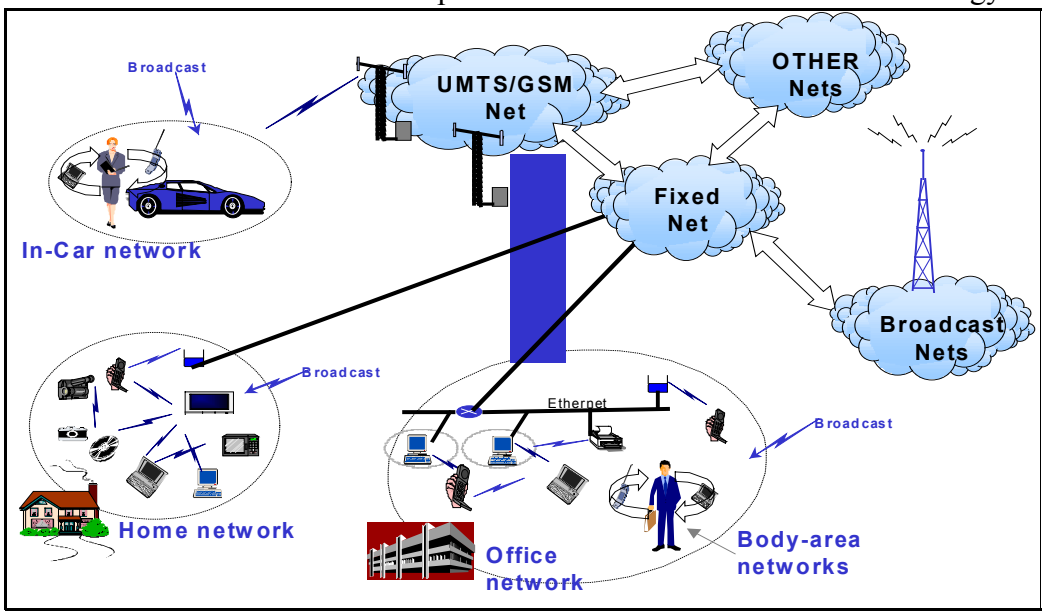

Figure 2 Distribution of devices in heterogeneous networks

4. Integration of Ad-hoc Networks into Cellular Networks

Future wireless communication will rely on different types of radio systems, for example satellite networks, high altitude platforms (HAPs), cellular networks (CN), point-to-multipoint (PMP) access systems, wireless local area networks (WLAN), and personal area networks (PAN). The most common and widely used wireless access systems today are cellular radio systems, based on GSM, GPRS and UMTS standards, and the recently deployed WLAN standards, e.g. IEEE802.11 and HIPERLAN/2. WLAN like systems can be run in an ad-hoc as well as in an infrastructure based mode. Unlike systems providing an ad-hoc mode, cellular systems rely on an infrastructure of base stations (BS) and require network planning and operation in licensed radio spectrums. UMTS provides cumulative data rates up to 2Mbit/s which might be still not enough for hot-spot areas where the number of mobile nodes (MNs) per area is very high. To increase the individual data rate of users, WLAN systems are introduced at these places, which can provide transmission rates of about 54 Mbit/s. These systems operate in unlicensed radio spectrums and, generally, offer mobile data communications with very low cost. Nevertheless, transmission power in such communication

systems is limited and hence the coverage is limited as well and interference between such systems is difficult to predict and to control.
Taking into account the advantageous, potentials and drawbacks of cellular network, WLAN, and self-organizing network architectures with respect to, e.g., coverage, capacity, mobility, cost of infrastructure and flexibility, it becomes obvious that a combination of them is the logical consequence for next-generation network concepts.
An evolutionary approach towards the architecture of a hierarchical multihop cellular network (HMCN) can be seen in Figure 3. An overlaying cellular mobile radio system, e.g. a 3G system, forms the basis of the proposed network architecture. The possible connection of each MN to a BS guarantees full coverage and this connection can always be taken as a fall back solution in the case that a MN looses connection to any other kind of network it might be connected to. This requires interoperability of existing networks and future networks and the support of vertical handover, i.e. handover between different wireless access networks (inter-system handover). The BS provides access to the backbone, which is most likely to be based on TCP/IP protocol suite.
In order to satisfy the increasing demand of higher data rates in hot- spot areas WLAN systems allow a broadband radio access to the Internet provided by access points (APs).
The next evolutionary step towards a hierarchical multihop network structure is to introduce multihop capable nodes (MHN), which can be fixed or even mobile, see Figure 3. With the fixed MHNs the coverage of the APs can be extended. At the same time fixed MHN can be connected to a power supply to offer more potent services. Sub-cells can be established in a self-organizing manner. This means the MHN recognizes its AP and takes over control functionality within the sub-cell. A typical control function comprises the management of the medium access within the sub-cell. Furthermore, it provides connections between MNs in the sub-cell, which can directly communicate with each other by means of a direct-mode. Moreover, the MHN and the MNs will be provided by signalling information by the AP, e.g., routing information. Besides the AP, signalling information can be provided by the overlaying cellular 3G system, too. Very interesting is also the case where the routing in the sub-cells is assisted by the overlaying 3G system.
Due to the proposed hierarchical structure an optimum control of resource allocation can be organized.
Besides fixed MHNs also mobile MHNs are considered in a further evolutionary step. In the case that the required data throughput cannot be provided any more by the AP or established fixed MHN, due to increasing penetration and/or to satisfy the future demands for packet-data services, a MN can become a MHN and establishes a sub-cell on demand. These cells can use the same or different frequencies. In this case sub-cells can be adaptively established. The spectral efficiency of the system can be enhanced when reusing the same frequency in different sub-cells. In the case of using different frequencies in different sub-cells the available transmission rate within the considered cell can be increased.

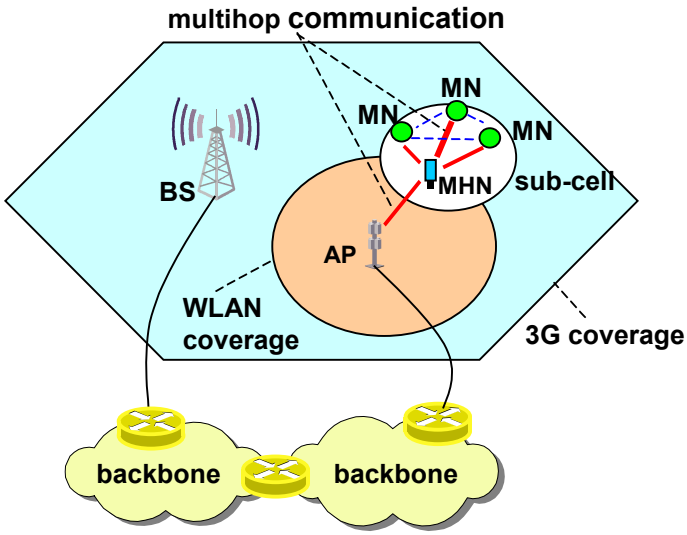

Figure 3: A Cellular Multihop Architecture

The spatial separation for the AP-MHN links is typically relative high, as one MHN supports a complete sub-cell of MNs with a respectively higher spatial dimension compared to a single MN. This simplifies the introduction of space division multiple access (SDMA) techniques at the AP due to the higher spatial separation between two sub-beams of the adaptive smart antenna. SDMA allows for simultaneous transmission and increases the spectral efficiency accordingly.

5. Distributed Antenna Concepts

The performance - with respect e.g. to throughput or delay - of ad-hoc networks is typically small compared to cellular systems. This is due to uncoordinated transmission on the air interface, protocol overhead for routing in high dynamic environments, transmission over multiple hops etc. It has been shown that the overall throughput in an ad-hoc network depends on the locality of the data traffic, i.e. if the traffic between different MNs is restricted to a small area or a few hops frequency reuse will improve capacity.

On the other hand enhanced forwarding techniques allow increasing the overall performance by a suitable combination of several MHNs to a so-called SFN (Single Frequency Network). SFNs are well known from broadcasting systems like DVB-T (Digital Video Broadcasting-Terrestrial) or DAB (Digital Audio Broadcasting) where large areas are supported by a number of base stations with the same frequency. SFNs are possible especially for OFDM (Orthogonal Frequency Division Multiplex) systems, whereby the guard interval has to be longer than the delay difference for the different BS-MN links.

In normal cellular systems SFNs are of no use, as each BS has to transmit communication data of different MNs. But in case of multihop communication several MHNs might be coupled for simultaneous forwarding of data in the same frequency band and at the same time. The MHNs are situated within the transmission range of an AP (Access Point), which broadcasts data – intended for the MN - in a first step to all MHNs as can be seen in Figure 4. In a second step the MHNs retransmit the data simultaneous to the MN.

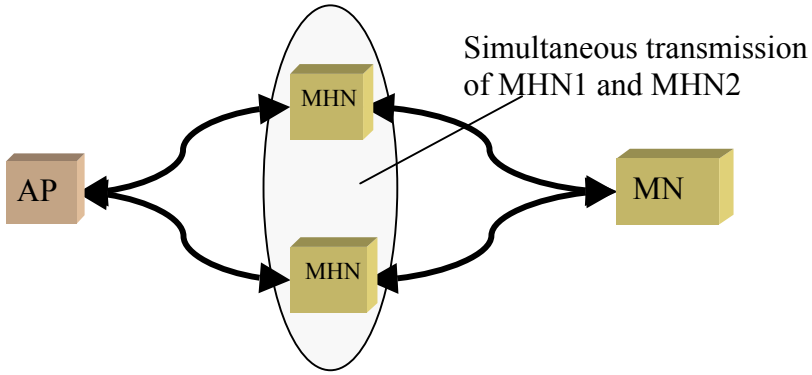

Figure 4: Typical SFN with two MHNs

The MHNs within the SFN network may be synchronized by the AP – i.e. all sub-carriers of the OFDM symbols are phase pre-distorted at the MHNs before forwarding - to guarantee constructive superposition of the MHN signals at the MN. With this concept significant performance improvements are possible, especially for high number of MHNs (see Figure 5). Additional advantages of SFNs are increased transmission range due to higher SNR and improved coverage as shadowing effects become less important. In case of mobile MHNs, the reliability is enhanced as the transmission between AP and MN can be continued even if one or several MHNs are switched of.

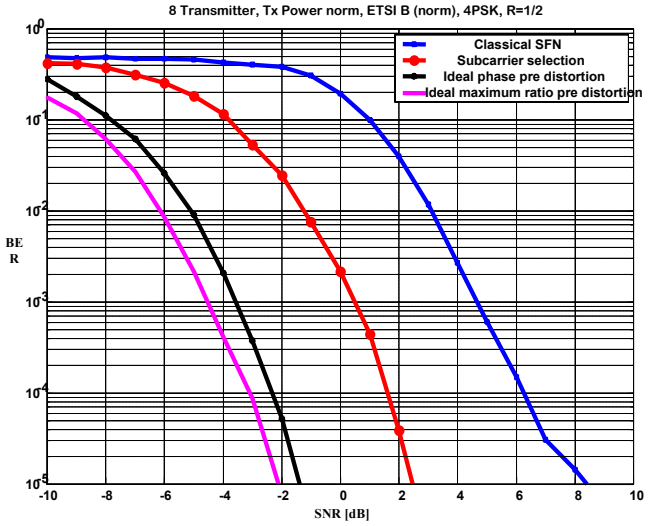

Figure 5 Performance gain for a SFN with 8 MHNs and different pre-distortion techniques for an ETSI B channel and normalized transmission power (QPSK, Code Rate 1/2). 'Classical SFN' is without and 'ideal phase pre-distortion' is with synchronization.

In a further step the MHNs of the SFN network might exchange information about their radio channels as can be seen in Figure 6. With this information optimised weighting factors can be calculated at each MHN before retransmission which results in a higher signal to noise ratio at the MN. This results in a higher overall throughput or less power consumption. Compared to simple phase pre-distortion additional gains are possible, as links with very small SNR values do not further disturb the receive signal at the MN.

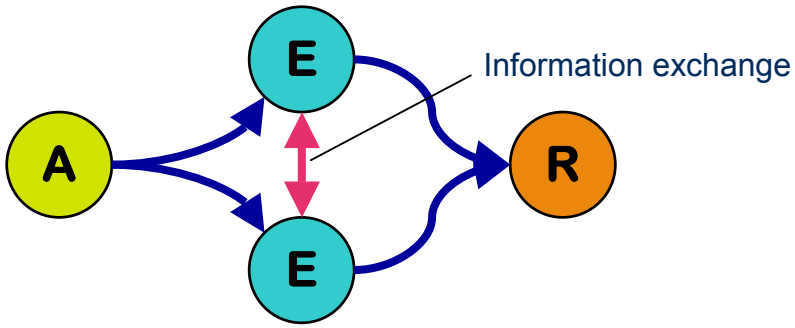

Figure 6 SFN with information exchange between MHNs

As an even more complex concept it is possible to cluster several MHNs or MNs in the vicinity of the AP (Access Point) and in the vicinity of the MNs to create two distributed MIMO antennas, e.g. to allow for SM (Spatial Multiplexing). The basic concept can be seen in Figure 7. The difference to standard MIMO antennas is, that there is no fixed wired connection between the different antenna elements, i.e. cluster of MHNs. But SM combines the signals of all receiving antenna elements to calculate the resulting data stream. These concepts require therefore the exchange of signalling data within the distributed antennas, e.g. about channel estimations. Optimal signalling concepts have to be defined and the trade-off between signalling protocol overhead and the resulting gain for distributed antenna systems has to be analysed.

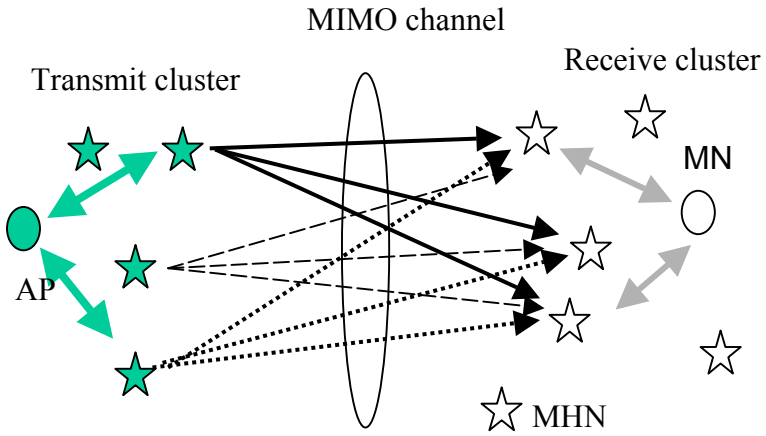

Figure 7 Concept for distributed smart antennas based on MHNs

Figure 8 shows an application of the distributed antenna concept in an ad-hoc network. In this case the MIMO channels are used to connect locally far apart parts of the ad-hoc network with high spectral efficiency, which improves the scalability of the overall network. Short distances, which span only very few hops, are connected by standard multihop connections.

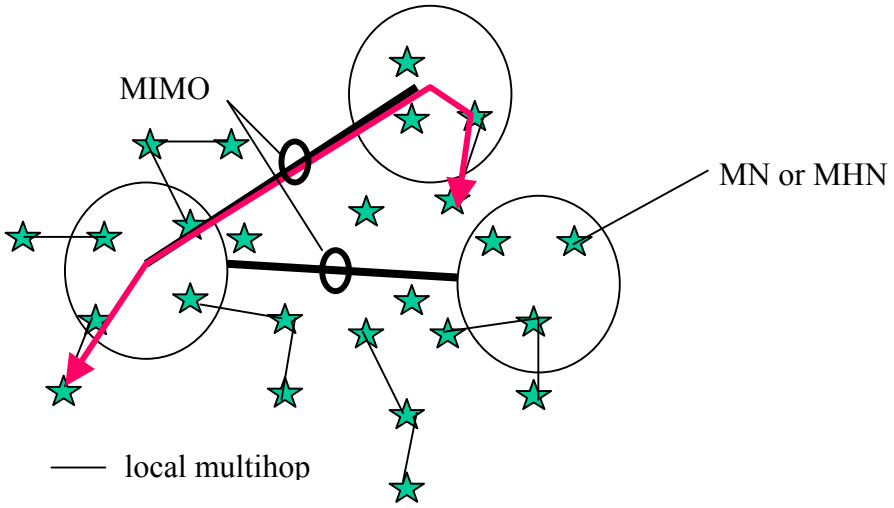

Figure 8: Hierarchical ad-hoc network with MIMO channels. The circles mark clusters of MHNs, which cooperate to form a smart antenna.

6. Network auto-configuration

Auto-configuration is a fundamental feature of ad-hoc networks. A node in an ad-hoc network has to detect other nodes in the network and to detect available services (provided by all nodes in the network not just by the neighboring nodes). The topology of an ad-hoc network changes frequently and nodes are joining, leaving or changing position in the network. An auto-configuration procedure has to ensure smooth and uninterrupted functioning of the network. If dedicated nodes are used (ad-hoc cluster with router to an overlay network), leaving the network by such a node can cause problems. The functionality of the leaving node has to be adopted by another node (assuming that there exists a node which supports this functionality). The configuration becomes easier if overlay nodes (no mobility, fixed routes) are used to span an overlay network. But this cannot be always assumed.
During the network formation phase, nodes have to agree on network topology (star, ring, point-to-point, point-to-multipoint, flat or layered hierarchy etc.). This will depend on the type of network (in a PAN, a personal communication control device will probably act as a master node in the network, while in a network comprising many PANs a fully connected and peer-to-peer network will be more suitable), underlying wireless technology (if Bluetooth is used then point-to-point or point-multipoint topology will be used) and application requirements.

7. Addressing

Addressing in ad-hoc networks is a specific problem. In the most of envisaged scenarios it is assumed that each node will have a unique IP address which is assigned automatically. In an IPv4 world it is not possible to allocate enough unique addresses for each small device envisaged by future networks. IPv6 probably have capacity for such allocation, but not every network will use an IP addressing scheme (in wireless sensor networks other sorts of addressing are proposed). On the other hand in contrast to IPv4, IPv6 is less efficient regarding the bandwidth efficiency. However, mechanisms for automatic address allocation in diversified networks are required.

A promising method based on Mobile IP [35], consists of a home address and a care of address that is build by using a distinct prefix for each subnet [36]. The locally assigned address could be used as care of address, whereas the unique home address could enable the Authentication, Authorization and hence the Accounting, similar to the IMSI (International Mobile Subscriber Identity) in GSM.

7.1. Address auto-configuration

The purpose of address auto-configuration mechanisms is the assignment of IP addresses that are easy to route with in the ad hoc network, therefore it has to be assured that each node in the network has a unique address.
One of the first solutions for ad hoc network address auto-configuration using IPv4 addresses has been proposed by Charles Perkins [28]. Addresses are randomly selected from a special part (169.254/16) of the network address space. Duplicated Address Detection (DAD) is used to eliminate duplicated addresses; this approach uses route discovery messages from a reactive routing protocol like DSR. DAD is performed only once per node. Hence, the uniqueness of addresses could not be guaranteed after merging two networks. This approach is not suitable for large ad hoc networks. The address space is limited to 2047 during and 655535 after the DAD. It should be considered that mobile nodes could have more than one interface to different networks, therefore may require multiple IP addresses.
Another approach, called Dynamic Registration and Configuration Protocol (DRCP), tries to modify DHCP to an auto-configuration protocol for wire and wireless networks. Therefore each node represents a DRCP client and server and owns an IPv4 address pool. The Dynamic Address Allocation Protocol (DAAP) is responsible for the distribution of the address pools. Each node requesting a pool gets half of the pool of a neighboring node. This results in a lot of unassigned addresses in an already scarce IPv4 address space. Also network merging is not considered.
Other approaches have been proposed e.g. IPv6 Stateless Address Auto-configuration (SAA), as a hierarchical solution working together with the LANMARK routing protocol, which is as well a hierarchical approach [29].
Further investigations will show if private IP addresses could be used as local subnet addresses, and the edge router can perform an address translation. Nevertheless the proposed addressing scheme is basically developed for IPv6, and future approaches have to be developed.

8. Routing

In ad-hoc networks a direct communication between any two nodes is possible subject to adequate radio propagation conditions and transmission power limitations of the nodes. If there is no direct link between the source and the destination nodes, multi-hop routing is used. If there is no infrastructure, each node, beside transmitting and receiving its own packets, takes an active part in establishing and maintaining routes for other nodes. A packet is forwarded from one node to another, until it reaches the destination. Of course, a routing protocol, run by all participating nodes, is required to discover routes between the source and the destination.
Routing in ad-hoc networks is a very challenging task due to several characteristics of ad-hoc networks and it has received a significant interest in the research community. Nodes are mobile, can join and leave network at any time and topology of the network can change quite rapidly, making routing tables obsolete. Since there is no centralized entity to keep the topology up-to-date, a distributed algorithm is required. Control information is exchanged between the nodes to capture the current state of the network. Another problem is caused by the nature of wireless communications. The bandwidth is limited and has to be used carefully. It is also susceptive to various interferences that can lead to sporadic connectivity patterns that can lead to establishment of

useless routes, low throughput and other problems. It is expected that the most of the nodes in an ad-hoc network will have limited energy resources. Hence, energy efficient routing protocols are required to minimize power consumption.

There are several routing protocols proposed for usage in ad-hoc networks. The main group of proposals comes from the work of IETF's MANET (Mobile Ad-hoc NETworks) group [3]. These routing protocols are designed for IP based, homogenous, mobile ad-hoc networks. Each node in the network has identical capability (identical communication devices and ability to perform functions from the common set of services). It is assumed that each node has a unique address (IP address for example). Number of hops is used as the only route selection criteria. Other parameters, like route delay, energy usage, fair distribution of power usage among terminals, load balancing or quality of service are not considered. These protocols focuses on fast route establishment and re-establishment and route maintenance with minimal overhead.

Two different approaches were taken in design of routing protocols for ad-hoc networks: proactive and reactive approach. Proactive protocols continuously update the topological view of the network by exchanging appropriate information among the network nodes and thus immediately know a route to a destination when required. The first routing protocols proposed for ad-hoc networks were proactive distance vector protocols. OLSR (Optimized Link State Routing) is a proactive protocol [3]. It is an optimisation of the classical link state algorithm tailored to the requirements of a mobile wireless LAN. The key concept used in the protocol is that of multipoint relays (MPRs). MPRs are selected nodes which forward broadcast messages during the flooding process. The content of the control messages flooded in the network is minimized, i.e. a node is not declaring all links to all neighbours, but just a small subset. That information is then used by the OLSR protocol for route calculation. The protocol is particularly suitable for large and dense networks as the technique of MPRs works well in this context.

The main problem of the proactive approach in ad-hoc networks stems from the fact that topology of ad-hoc networks is changing continuously. Hence, a frequent dissemination of topology information is required which causes a large routing overhead. Also, depending on the traffic pattern in the ad-hoc network, it is possible that only a small fraction of routes is used. This effectively means that already constrained wireless and computing resources were wasted.

AODV and DSR are examples of reactive or "on demand" routing protocols [4], [5]. These protocols do not continuously maintain the overall network topology. Topology is maintained only for those routes that are in use. When a route is not used anymore it is removed from routing tables. The network is flooded with "route request" messages when a new route is required. When a "route request" message is received by the destination or a node which has a route to the destination, a "route reply" message is generated and unicast back to the source node. Various simulations have shown that on-demand protocols perform better in ad-hoc networks then table-driven protocols [9]. The first real world implementations of these protocols were deployed recently [6], [7], [8].

The initial tests were done in small (up to 10 nodes), WLAN (802.11 and 802.11b) based networks, with usually static nodes. It is shown that route latency in observed scenarios ranges from 2-3ms for 2 hops up to 70ms for 4 hops. For many applications this is acceptable. Poor performance of TCP in wireless networks is confirmed and the necessity of TCP modifications for use in wireless domain is reaffirmed. Available throughput decreases with the number of hops. On 2 hop routes up to 2 or 3Mbit/s can be expected, while 4 hop routes provide around 1mbit/s.

All implementations are assuming a broadcast wireless medium and are using "Hello" messages to announce the presence of individual nodes to other nodes. It is proved that this mechanism is not reliable in all circumstances and can be a cause of frequent route breakages and poor network performance. Although utilization of the link layer information is proposed in protocols it is still not implemented due to problems with hardware, firmware and device drivers capabilities.

It still has to be explored how will these protocols perform in Bluetooth or UWB networks. Bluetooth networks are organized in piconets and scatternets. Although when IP is deployed over

the Bluetooth layers a broadcast medium for users of IP services is provided, the underlying communication is always routed via master nodes of piconets. As the master node knows which nodes are participating in the piconet that information could be used for improvements of routing algorithms in Bluetooth networks. This will require cooperation of IP based routing protocols with Bluetooth layers.

UWB (Ultra Wide Band) is another wireless technology that will likely be used in ad-hoc networks. This technology provides good position location of communicating nodes and that information could be used to support efficient routing in ad-hoc networks as proposed in [10].

As the most of devices in ad-hoc networks are battery driven, power consumption is very important and should be minimized in order to maximize the battery life. CPU, data storage and user interface are consuming power, but wireless transmission is still the main power consumer. The required energy for a successful transmission decreases rapidly with decrease of distance (typically with 4-th order of magnitude). If transmit power control is implemented, then depending on the distance, multi-hop routes could be more energy effective than one hop route, even when direct communication is possible. However, the existing protocols do not use this feature. It is assumed that maximum power is always used and the number of hops is used as the only criteria. Hence, the expended energy in current implementations of routing protocols can be much higher than the minimum energy required.

It was also noticed that significant energy is consumed even when there is no data traffic in the network due to the power consumed for continuous listening to wireless medium [11]. Introducing a "sleeping" mode in which nodes consume minimal power can help in solving this problem. However, "sleeping mode" introduces additional latency in the network and can cause increase in signalling overhead. Delays and signalling overhead can have a detrimental effect on overall network performance. A trade-off between energy savings and routing efficiency is required.

Several protocols for power-aware routing in ad-hoc networks have been proposed. Power aware metric is introduced in [12] and an appropriate routing algorithm that minimizes this metric is proposed. MAC layer modifications that power down inactive nodes are also suggested. Another proposal [13], uses transmit power adjustments to control the topology of a multi-hop network. In [14], a distributed position based protocol that uses location information to compute the minimum power relay route to the destination, which minimizes the energy consumed for routing the packets is proposed.

Routing in wireless sensor networks has different requirements then routing in MANET like ad-hoc networks. A wireless sensor network is comprised of many small devices, capable of sensing, computing and with a wireless access. The nodes in a wireless sensor network are usually not mobile, but changes in topology are possible due to battery depletion or malfunction of certain nodes. It is not expected that each sensor will have a unique address. The energy resources of sensor nodes are very limited and a great care of power consumption has to be taken. The information flow pattern is much different comparing to Manet network. In each sensor network, a so-called "sink node" is envisaged, which represents a user node or a gateway to a wide area network. Sensing results are, after some processing, transmitted from sensors to the sink node. Hence, routing protocols in this environment are mainly concerned with establishment and maintenance of routes between sensors and a sink node in the network. User's query will not be addressed to a specific sensor but will be disseminated through the network until it reaches a group of sensor that has the answer (user will ask for the temperature in south-west part of the forest, not the temperature measured by a specific sensor). The main body of wireless sensor networks research is based in USA and is funded by the DARPA. Several routing protocols specifically developed for sensor networks are proposed [15], [17], [16].

9. Security

High-level security requirements for ad-hoc networks are basically identical to security requirements for any other communications system, and include: authentication, confidentiality, integrity, non-repudiation, access control and availability. However, similar to wireless communication systems putting additional challenges for implementation of above mentioned services when compared to fixed networks, ad-hoc networks represent even more extreme case, requiring even more sophisticated, efficient and well designed security mechanisms. These additional challenges are caused by two basic assumptions of an ad-hoc system: complete lack of the infrastructure, and a very dynamic and ephemeral character of the relationships between the network nodes.

The lack of infrastructure implies that there is no central authority, which can be referenced when it comes to making trust decision about other parties in the network and that accountability can not be easily implemented. The transient relationships do not help in building trust based on direct reciprocity and give an additional incentive to nodes to cheat.

Ad-hoc networks rely on cooperation of involved nodes in order to build and maintain the network. Current versions of mature ad-hoc routing algorithms only detect if the receiver's network interface is accepting packets, but they otherwise assume that routing nodes do not misbehave. Whereas such an assumption may be justified when single domain networks are concerned, it is not easy to transpose it on a network consisting of nodes, unknown to, and not trusted by each other. Since ad-hoc networks use multi hop routing protocols, where each of the nodes in addition to its own packets has to forward packets belonging to other nodes, selfish behaviour may represent a significant advantage for a node, saving his battery power and reserving more bandwidth for its own traffic. However, if a large number of nodes start to behave non-cooperatively, the network may break down completely, depriving all users of the services. Non-cooperative behaviour in multi hop routing protocols may also result in a denial of service attacks on the network, where the malicious nodes join the network for a sole reason of misbehaving and depriving all other nodes of legitimate services. Such denial-of-service focused misbehaviour may consist of dropping (not forwarding) the packets, injecting incorrect routing information, replaying expired routing information or distorting routing information in order to partition the network. Also bogus nodes may try to attract as much traffic as possible to them in order to be able to analyse it. In general, attacks on a routing protocol can be classified as dropping of data packets, route modifications, dropping of error messages and frequent route updates.

One of the most commonly mentioned security problems in wireless network environment is confidentiality of transported data, i.e. eavesdropping problem. However, this concern is vastly exaggerated, and can be easily solved once the authentication and key sharing mechanisms are in place. Similar considerations apply to the integrity protection, with integrity of the data stored in the devices being the most challenging issue.

Mobile, battery powered, devices always provide a constrained computational environment, when compared to fixed terminals. This is especially true in case of small wireless sensing devices and distributed personal networks. Also embedded intelligence and ubiquitous computing applications, even if free of power consumption considerations, will require cheap processors, with limited computational abilities. The small processors are often too slow for computationally intensive public-key cryptography. In mobile environment, solving this problem by means of pre-computation or background task is not a solution, since the battery capacity puts an ultimate limit on an amount of computation which devices can perform. Thus, for the battery-powered devices, the most relevant performance figure is no longer bits per second, but bits per joule.

One of the biggest challenges in the area of confidentiality is not protecting the data transported by the network, but protecting the data stored on a device itself. Building tamper resistant and cost effective devices has turned up to be a challenge, with most of the portable devices providing low

security against data extraction. Smart card industry has driven most of the research in the area of tamper resistance, with some remarkable results. The problem of tamper resistance is especially valid in case of devices located outside of the direct control of the owner, e.g. wireless sensors. The extracting of the information stored in the device may lead to both compromise of user's privacy and to impersonation attacks. The extracted authentication information from a remote sensor may enable an impostor to send the false sensing information or to block sending of the correct data. These kinds of attack can be avoided to some extent by using redundant information sources and communications routes and by applying voting mechanisms.
Another challenge is metadata protection, including confidentiality of identity (pseudonymity and anonymity), confidentiality of location (traceability) and traffic analysis. The confidentiality of this metadata will gain on importance in the ubiquitous computing environment, where the ubiquitous computing infrastructure could potentially become a tool for a powerful surveillance, making us involuntary participants in a worldwide "Big Brother" show.
The most common attacks on wireless communication systems consist of jamming the communication channel. This area has been studied intensively for military applications and most of the results can be applied also to civil networks.
The more dangerous attack in civil applications, typically using an open ad-hoc environment, may consist of so-called "sleep depravation torture". In this type of denial-of-service attack, attacker is trying to deprive a device of battery power, by keeping it awake and engaging in the communication all the time. Strong authentication of communication peers or some kind of accountability, based on either expensive pseudonyms and reputation mechanisms or micro-payments, could be used to prevent to some extent this kind of attack. Micro-payments could have form of both fungible payments, having monetary value, or in fungible payments, e.g. crypto puzzles. In more advanced scenarios, infungible micro-payments could be harvested in order to perform some useful computations in a distributed way, similar to SETI@home concept.
Data freshness is a security consideration in some applications, too. This applies to freshness of both application data (e.g. sensor readings) and freshness of signalling information (e.g. time synchronization within the network).
Information in ad-hoc networks is likely to traverse via various nodes over which end-users do not have control nor have an established trusted relationship. Trust establishment and end-to-end security in a highly vulnerable wireless space will have to be provided.

10. Service discovery

The environment of the future will be saturated with intelligent devices providing various information and services, and forming different networks. Depending on location and context, a user will require access to information or services. A protocol that can abstract a great variety of networks and can efficiently and seamlessly discover location based and context aware services is required.
A protocol must also enable discovery of services between devices, which are not directly connected, but are present within a multihop ad-hoc network. An efficient protocol should be capable of not leaving services and infrastructure underutilized. It should first identify the existence of a service, then decide if the existent technology can bind to it, and finally establish successfully a session. In order to do that, it should be capable of giving the ability to the devices to announce their presence to the network and describe their capabilities. As well as this, it should discover every available service in the network and make automatically the configuration needed. It should also be independent of the transmission protocol as in complex networks, different transmission protocols are expected to be operating simultaneously.

Many protocols have been developed and proposed as a solution to the service discovery problem, which are based on the service discovery methods: centralized and distributed pull, and distributed push. By centralized pull, clients pull the services whenever needed from a central component (called Central Registry) where all the existent services in the network are registered, by distributed pull they pull services from the network itself, and by distributed push, service providers push information concerning the services to the network.
'Universal Plug `n Play' uses the distributed pull method, relies on HTTP and TCP/IP and can provide leasing and eventing. Its main drawback is that it supports only known devices and that it does not support many network configurations. 'Jini' is a Java based Service Discovery Protocol and uses the centralized pull method. It also provides eventing and leasing, and it uses a directory-centric approach. Its main disadvantages are that it does not support many network configurations, and that its centralized service discovery is not suitable for ad-hoc networks. 'Salutation' supports both centralized and distributed service discovery, transport independent addressing, and device capability exchange. It is designed to function in pervasive, and heterogeneous networks and above of the most network protocols. Its main problems are that no leasing is supported, and that the addressing is complex. IBM DEAPspace supports the distributed push method and the service description is fulfilled with strings and XML. Its main drawback is its word view of services and its emphasis on devices.
Above-mentioned wired networks proposals have to be adapted for the wireless world and especially for the high dynamic in ad-hoc networks. Due to the high dynamic, the user might switch off server that announces services, so the information has to be stored at several servers. Information might be flooded into the network, which causes high overhead. So appropriate strategies have to be investigated which may include hierarchies for service distribution and announcement.

11. Authentication, Authorization and Accounting

As a wide variety of distributed devices and services will be carried and used by individuals in the future, and many of these devices and services will act autonomously without user intervention and consent, it will be important to restrict access to secure information, to authenticate users, and to enable charging for provided services. Similar procedures exist today, but are used in an organized fashion, by users and servers with an established relationship. The environment in future networks will be much more dynamic, with many more users and service providers, and it is not feasible for a user to require a separate user name and password for every service he/she intends to use. Numerous micro-authentications and micro-payments will have to be performed seamlessly and unobtrusively (like in ISTAG's Scenario 3), based on high-level user-defined policy.

12. Air interfaces

The air interface requirements for ad-hoc networking are many and varied. This can range from very low power, low data rate telemetry and sensor requirements, where a small battery may be required to give over 10 years of connectivity, to very high data rates for high quality multimedia distribution in home.
Common requirements include coexistence between multiple instances of the same air interface (in the same, or collocated ad-hoc networks) and any other air interfaces (ad-hoc or deployed).
To reach the requirements, techniques for dynamic frequency selection (DFS), link adaptation and power control have to be included, like in the recent standardized systems HiperLAN/2 or IEEE

802.11. Furthermore, techniques to support QoS have to be added. Current efforts for QoS support in pure ad hoc networks lead to establishment of a central controller (e.g. IEEE 802.11e). Techniques to address this issue include furthermore dynamic resource allocation, spectrum sharing and spectrum overlay.

MAC (Medium Access Control) layer issues

The MAC layer has to provide efficient and fair access to the wireless medium for all devices and to ensure reliable data transmission. Current MAC protocols for ad hoc networks could be classified in three groups, depending on their channel access strategy: contention protocols, allocation protocols, and a combination of both - the hybrid protocols.
Contention protocols use similar protocols like ALOHA or CSMA, with the exception of slotted ALOHA. The most contention protocols are based on asynchronous communication models. Collision avoidance is an important feature of these protocols that is realized through some form of control signalling. It has been shown that contention protocols are simple and tend to degrade as the traffic load increases, whereby the number of collisions rises. In overload situations a contention protocol can become unstable as the channel utilization drops. This can result in exponential increase of packet delay and the network service breakdown, since few, if any, packets can be successfully exchanged.
Allocation protocols employ a synchronous communication model and use a scheduling algorithm that generates a mapping of time slots to nodes. The mapping results in a transmission schedule that determines in which particular slots a node is allowed to access the channel. This effectively leads to a collision free transmission schedule. It turns out that the allocation protocols tend to perform well at moderate to heavy traffic load but these protocols are disadvantaged at low traffic due to the artificial delay induced by the slotted channel.
Hybrid protocols can be loosely described as any combination of two or more protocols.
Nowadays the contention protocols are well known and used by the most projects investigating ad hoc routing issues.
The multiple access with collision avoidance (MACA) [30] protocol uses a handshaking dialogue to reduce the hidden node interference and minimize the number of exposed nodes. This handshake consists of a request-to-send (RTS) control packet sent from a source node to its destination and a clear-to-send (CTS) control packet sent by the destination. On reception of CTS packet the source node can transmit its packet. Further enhancements are introduced by the MACAW [31] protocol. The MACAW protocol includes carrier sensing to avoid collisions and positive acknowledgements. Improvements are also made to the collision resolution algorithm to ensure a more equitable sharing of the channel.
A very similar approach to MACAW is used in the distributed coordination function DCF of the IEEE 802.11 standard, improved with collision avoidance [32]. Nodes deliver data packets of arbitrary lengths (up to 2304 bytes), after detecting that there is no other transmission in progress. However, if two nodes detect the channel as free at the same time, a collision occurs. IEEE 802.11 defines a collision avoidance (CA) mechanism to reduce the probability of such collisions. As part of CA, before starting a transmission, a node performs a back-off procedure. It keeps sensing the channel for an additional random time after detecting the channel as being idle for distributed coordination function inter-frame space (DIFS).

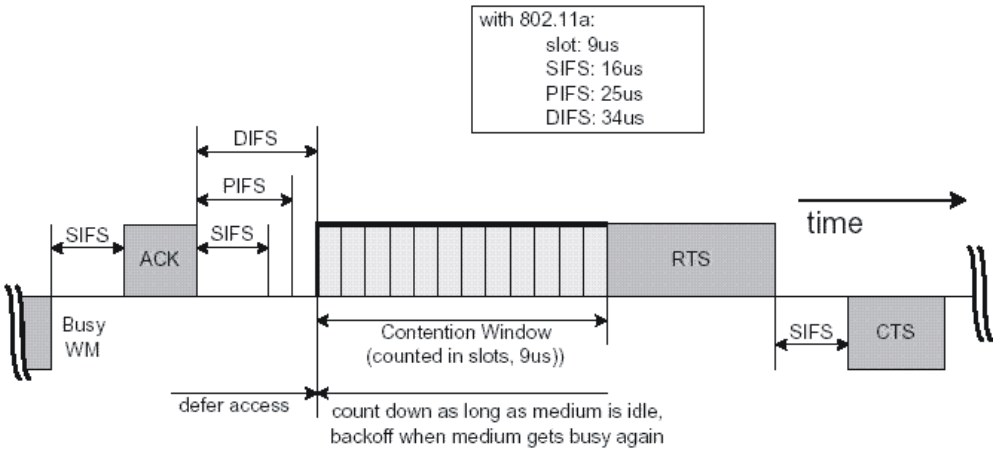

Figure 9 Inter-frame Space and back-off sequence

Only if the channel remains idle for this additional random time period, the node is allowed to initiate the transmission. The duration of this random time is determined as a multiple of a slot time (e.g. 9μs in 802.11a) uniformly distributed between zero and Contention Window (CW), which is a counter, maintained by each node. Figure 9 shows an example: After a successful transmission, a node starts transmission, since the channel has been idle for a duration of DIFS and the following back-off slots.

The CW size increases when a transmission fails, i.e., the transmitted data frame has not been acknowledged. After any unsuccessful transmission attempt, another back-off is performed with a doubled size of the CW. This reduces the collision probability in case multiple nodes are attempting to access the channel. The nodes that deferred from channel access during the channel busy period do not select a new random back-off time, but continue to count down the time of the deferred back-off in progress after sensing the channel as being idle again. Therefore nodes, that deferred from channel access because their random back-off time was larger than the back-off time of other nodes, are given a higher priority when they resume the transmission attempt. After each unsuccessful transmission attempt, the CW is doubled until a predefined maximum CWmax, (e.g. 1023 for 802.11a) is reached. After a successful transmission, the CW is reset to CWmin and another random back-off is performed by the transmission-completing node, even if there is no other pending data packet to be delivered. This is called post-back-off, as this back-off is done after, not before, a transmission (Figure 10).

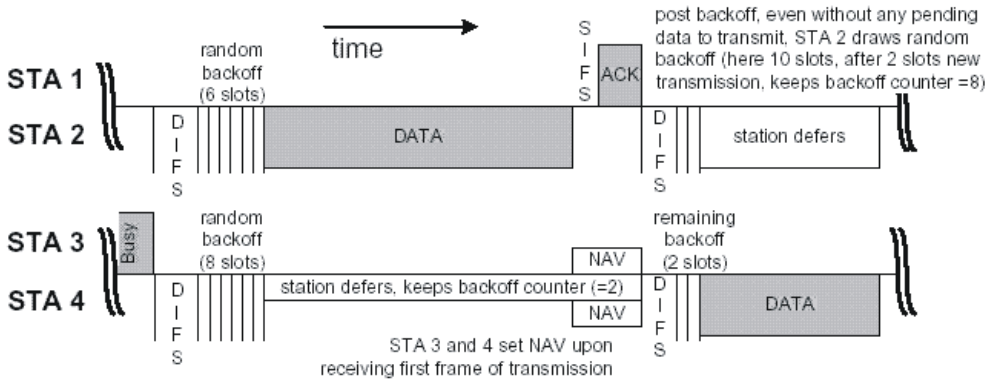

Figure 10: After every transmission a node has to perform another back-off, the post-back-off. This happens irrespective if the node has pending data to transmit or not.

There is one situation when a node is not required to perform the random back-off before starting data transmission. An data packet arriving at the STA from the higher layer may be transmitted

immediately without waiting any time, if the last post-back-off has been finished i.e., the queue was empty, and additionally the channel has been idle for a minimum duration of DIFS. All the following data packets after this packet have to be transmitted after random back-off, until the transmission queue is empty again.
Investigations have shown drawbacks of 802.11 MAC protocol in multi-hop communication. Especially the optimisation in terms of routing could be improved, by providing some of the information available (SNR info, packet acknowledgments, etc.) at MAC layer to ad-hoc routing protocol on the network layer. Furthermore connectivity on MAC level has to be assured because of the IP address assignment problem.
In case of multihop communication the POH (Protocol Overhead) becomes an important issue. The MAC frame has to assure that:

- The resource requests are handled as far as possible at the MHNs without involvement of an AP (in case of infrastructure mode);
- The transmission between the AP and the MHNs is synchronized as far as possible;
- QoS can be guaranteed for the complete multihop link;
- TTAs (Transceiver Turn Around Times) are minimized.

Multiple heterogeneous physical layers in one network

With such a large number of various devices it is to be expected that not all devices in an ad-hoc network will have the same physical layer. Appropriate protocols are required to bridge between the networks. Service discovery, routing, and other protocols will have to work in such a diversified environment. Load balancing is also an important issue for heterogeneous networks; an ISP may decide to relieve his GPRS network by using multiple WLAN hops.
It has to be investigated, whether SDR (SW Defined Radio) techniques can help to adapt to a fast changing environment.

13. Conclusions

In conclusion ad-hoc technology is a viable solution where only a missing or incomplete infrastructure exists. There are a lot of problems to be solved to make ad-hoc an efficient and powerful technology. In dependency on the network structure and application the problems (such as routing, security, addressing, and MAC design) differ. The paper addresses some of these problems and gives first solutions.

14. References

[1] Book of Visions, Wireless World Research Forum
[2] Scenarios for Ambient Intelligence, EU IST Advisory Group
[3] MANET Working group, http://www.ietf.org/html.charters/manet-charter.html
[4] C.E. Perkins, E.M. Royer, S.R. Das, "*Ad-hoc On Demand Distance Vector (AODV) Routing*", IETF Internet Draft, draft-ietf-manet-aodv-10.txt, January 2002 (work in progress)
[5] D.B. Jonhson, D.A. Maltz, Yih-Chun Hu, J.G. Jetcheva, "*The Dynamic Source Routing Protocol for Mobile Ad-Hoc Networks (DSR)*", IETF Internet Draft, draft-ietf-manet-dsr-07.txt, February 2002 (work in progress)
[6] D.A. Maltz, J. Broch, D.B. Jonhson, "*Experiences Designing and Building a Multi-hop Wireless Ad-hoc Testbed*", Technical Report CMU, CMU School of Computer Science

[7] S. Desilva, S. R. Das, "*Experimental Evaluation of a Wireless Ad-Hoc Network*", Proc. of the 9th Int. Conf. on Computer Communications and Networks (IC3N), Las Vegas, October 2000.

[8] M. Dupcinov, M. Jakob, S. Murphy, S. Krco, "*An Experimental Evaluation of AODV Performance*", submitted to Mobicom 2002

[9] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, J. Jetcheva, "*A Performance Comparison of Multi-Hop Wireless Ad-Hoc Network Routing Protocols",* Proc. of the Mobicom 98, October 25-30 1998, Dallas, Texas, USA.

[10] S. Capkun, M. Hamdi, and J. P. Hubaux, "*GPS-free Positioning in Mobile ad-hoc Networks*," Proc. 34th Annual Hawaii Int. Conference on System Sciences, January 2001.

[11] Y. Xu, J. Heidemann, D. Estrin "*Adaptive Energy-Conserving Routing for Multihop Ad-Hoc Networks*", Research Report527, USC/Information Sciences Institute, October, 2000.

[12] Singh, S., Woo, M., and Raghavendra, C.S., "*Power aware routing in mobile ad-hoc networks*", *Proc. of MOBICOM*, 1998, pp.181–190.

[13] Ramanathan, R., Rosales-Hain, R., "Topology control of Multihop Wireless Networks using transmit power adjustment", IEEE INFOCOM 2000, pp. 404–413.

[14] Roduplu, V., Meng, T., "*Minimum energy mobile wireless networks*", *IEEE JSAC*, v. 17, n. 8, Aug. 1999, pp. 1333-44.

[15] C. Intanagonwiwat, R. Govindan, D. Estrin, "*Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks*", Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCOM '00), August 2000, Boston, Massachussetts.

[16] D. Braginsky, D. Estrin, "*Rumor Routing Algorithm For Sensor Networks*", Proc. of the International Conference on Distributed Computing Systems (ICDCS-22), November 2001.

[17] Y. Yu, R. Govindan, D. Estrin, "*Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks*", UCLA Computer Science Department Technical Report UCLA/CSD-TR-01-0023, May 2001

[18] Sonja Buchegger, Jean-Yves Le Boudec, "*The selfish node: Increasing routing security in mobile ad-hoc networks*", Research Report RZ 3354, IBM Research, Zurich Research Laboratory, 8803 R¨uschlikon, Switzerland, May 2001.

[19] Levente Buttyan, Jean-Pierre Hubaux, "*Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad-hoc networks*", Tech. Report DSC/2001/001, Institute for Computer Communications and Applications, Department of Communication Systems, Swiss Federal Institute of Technology, Jan. 18 2001.

[20] Jean-Pierre Hubaux, Levente Buttyan, Srdan Capkun, "*The quest for security in mobile ad-hoc networks*", Proceedings of the ACM Symposium on Mobile Ad-hoc Networking and Computing (MobiHOC) (Long Beach, CA), ACM, Oct. 2001.

[21] Thomas Kuhn, "*Security architecture for future mobile terminals and applications*", Interim Report SHA/DOC/SAG/WP2/D03/2.0, IST-2000-25350 - SHAMAN, November 2001, Available online at: http://www.ist-shaman.org.

[22] Sergio Marti, T. J. Giuli, Kevin Lai, Mary Baker, "*Mitigating routing misbehavior in mobile ad-hoc networks*", Mobile Computing and Networking, 2000, pp. 255-265.

[23] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler J. D. Tygar, "*SPINS: Security protocols for sensor networks*", 7th ACM International Conference on Mobile Computing and Networking (Rome, Italy), vol. 1, ACM Press, 2001, pp. 189-199.

[24] Roland Schmitz, "*Results of review, requirements and reference architecture*", Interim Report SHA/DOC/SAG/WP1/D02/1.1, IST-2000-25350 - SHAMAN, December 2001, Available online at:http://www.ist-shaman.org.

[25] Frank Stajano, Ross Anderson, "*The resurrecting duckling: Security issues for ad-hoc wireless networks*", 7th International Workshop on Security Protocols (M. Roe B. Crispo, ed.), Lecture Notes in Computer Science, Springer Verlag, 1999.

[26] Seung Yi, Prasad Naldurg, Robin Kravets, "*Security-aware ad-hoc routing for wireless networks*", Technical Report UIUCDCS-R-2001-2241, UIUC, 1304 West Springfield Avenue, Urbana, IL 61801-2987, USA, Aug. 2001.

[27] Lidong Zhou, Zygmunt Haas, "*Securing ad-hoc networks*", IEEE Network Magazine 13 (1999), no. 6.

[28] Charles E. Perkins, Elizabeth M. Royer and Samir R. Das, "*IP Address Autoconfiguration for Ad Hoc Networks*", 2000, Internet Draft:draft-ietf-manet-autoconf-00.txt, expired

[29] K.Weniger, M. Zitterbart: "*IPv6 Autoconfiguration in Large Scale Mobile Ad-Hoc Networks*", Proceedingsof European Wireless 2002, Florence, Italy, Feb 2002

[30] P.Karn, "*MACA – A new channel access protocol for packet radio*", Prc. ARRL/CRRL Amateur Radio 9th Comput. Networking Conf., Sept. 22, pp. 134-140,1990

[31] Ivan Stoijmenović, "Hanbook of Wireless Networks and Mobile Computing", Wiley-Interscience, 2002

[32] IEEE 802.11. Draft Supplement to STANDARD FOR Telecommunication and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part11: Wireless Medium Access Control (MAC) and physical layer (PHY) specification: Medium Access Control (MAC) Enhancements for Quality of Service (QoS). Draft Supplement to Standard IEEE 802.11, IEEE, New York, November 2001

[33] IEEE. Supplement to Standard [for] Information Technology-Telecommunications and information exchange between systems-Load and metropolitan area networks-Specific Requirements – Part11: Wireless LAN Medium Acces Control (MAC) and Physical Layer (PHY) specification: High Speed Physical Layer in the 5Ghz Band. Standard IEEE 802.11a, IEEE, New York, 1999

[34] S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz, L. Stibor. "IEEE 802.11e Wireless LAN for Quality of Service", In European Wireless 2002, 2002

[35] C. Perkins, " IP Mobility Support", IETF RFC 2002, 1996

[36] J. Xi, C. Bettstetter, "Wireless Multihop Internet Access: Gateway Discovery, Routing, and Addressing", Proc. World Wireless Congress, San Francisco, USA, 2002

15. Potential participants

Organization	Contact Person	Research Area
Aalborg University, Denmark		
Acticom, Germany	Frank Fitzek	
Aachen University of Technology, ComNets, Germany	Bernhard Walke	
Athens UEB, Greece	George Polyzos	
Carleton University, Canada	Halim Yanikomeroglu	
CEA-LETI, France	Jean-René LEQUEPEYS	
Ericsson Systems Expertise, Ireland	Srdjan Krco	
Fujitsu Laboratories, UK	Seshaiah Ponnekanti	
IBM Research, Switzerland	Pierre R. Chevillat	
ICN Siemens, Germany	Wolfgang Zirwas	
KTH, Sweden		
Mitsubishi Electric ITE, France	Laure SEGUIN	
Motorola		
Nokia, Finland		
Nortel Networks, UK	Andy Jeffries	
Philips, UK	Bernard Hunt	
Telecommunications Technological Center of Catalonia, Spain	Carles Anton Haro	
TID, Spain		
TU Dresden, Germany		
TU Ilmenau, Germany		
UPC, Spain	David Remondo	MAC and network level
VTT, Finland		