An Overview on Ad Hoc Networks

Martinus Dipobagio
Institute of Computer Science (ICS), Freie Universität Berlin
Email: dipobagi@inf.fu-berlin.de

***Abstract*—The wireless ad hoc networks consist of a collection of wireless nodes, that communicate over a common wireless medium. The nodes communicate without an infrastructure, such as base station, wired access point, etc. The establishment of the networks must be in a distributed and decentralized manner. Therefore, the complexity of the networks is in the nodes self. The nodes must be able to solve network's problem, such as routing and security. Despite the technical challenges, the interests of the ad hoc networks increase rapidly in recent years, because they support mobility and are very well suited for many difficult situations, such rescue mission, military, vehicular communications, etc. In this overview article, I introduce the concept of wireless ad hoc networks and specially mobile ad hoc network (MANET), their architecture, purposes, applications, advantages, disadvantages, and comparison with infrastructure networks.**

I. Introduction

Wireless ad hoc networks are collections of wireless nodes, that communicate directly over a common wireless channel. The nodes are equipped with wireless transceiver. They don't need any additional infrastructure, such as base station or wired access point, etc. Therefore, each node doesn't only plays the role of an end system, but also acts as a router, that sends packets to desired nodes.

The ad hoc are expected to do assignments, which the infrastructure can't do. Ad hoc networks are mostly used by military, rescue mission team, taxi driver. Their works can't rely on a infrastructure's network. As an illustrative example, imagine firefighters put out hazardous fire in a big forest. They have to communicate each other, but establishing a infrastructure or cabling in such area is impossible or too expensive.

The main problems in ad hoc networks are routing and characteristic of wireless communication. In infrastructure's networks a node can communicate with all nodes in the same cell. In ad hoc a node can communicate only with nodes in its area. this node can communicate with other nodes, but a routing algorithm is necessary. Unlike wired communication, wireless networks have transmission problem with data transmission such as, possibility of asymmetric connections and higher interferences.

The aim of this overview article is to provide informations on ad hoc networks and specially MANET, their structure, their applications on the current time, as well as their strong and weakness in comparison with infrastructure networks. Section 2 introduces ad hoc's architecture and its uses. Section 3 explains which components ad hoc networks need, so that a ad hoc network can be established. Section 4 discusses the goals of the networks. Section 5, 6, and 7 review the advantages, disadvantages, and comparison of the networks respectively. Finally, section 8 concludes of the overview article.

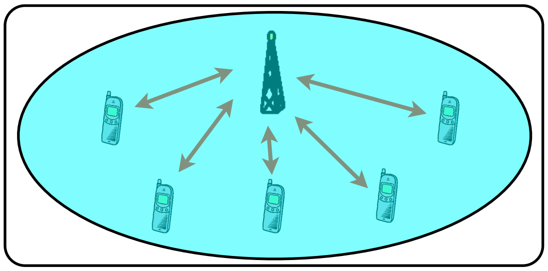


Figure 1: Cellular Network

II. Ad Hoc Network Overview

The word ad hoc is from Latin and means “for this (only)”. In the case of computer networks, the ad hoc networks mean wireless network without infrastructure, they can be called spontaneous network.

One Way to understand ad hoc networks is by comparing them with infrastructure based wireless networks, such as cellular network and WLAN. In the infrastructure based wireless networks a node can only send a packet to a destination node only via access point (in cellular network like GSM, it is called base station). The access point establishes an network area and only the nodes in this area can use access point's services. There are some unknown events, which cause access point's malfunction. The nodes lose their network and they are quasi not working. It is the biggest infrastructure's disadvantage.

There are also some reasons to sacrifice or not to use access point's services. These can be cost factor, impossibility to install access point in short time, etc. In this case the nodes have to build its own network. This network is called wireless ad hoc network.

The wireless ad hoc networks only consist of nodes equipped with transceiver. The network are created to be independent from an infrastructure. Therefore, the nodes must be able to arrange their own networks. Keep in mind, that a node can now communicate only with other nodes in its transmission range. In the infrastructure based wireless network, the nodes can communicate with a node, which is located in another network area, by transmitting data to destination access point and this access point relay the data to the desired node.

It seems like, that the ad hoc networks are not powerful enough. Each node has its own transmission range, if these small transmission areas are combined, they will form a much bigger transmission area. The nodes transmit their data with

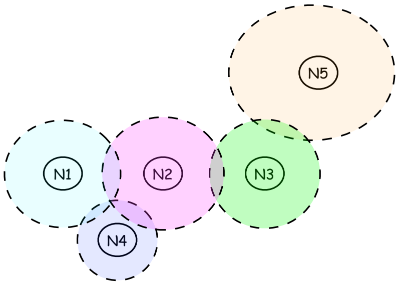
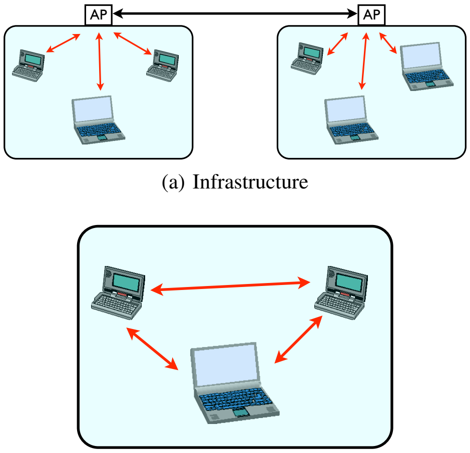


Figure 2: Transmission area in ad hoc



(a) Infrastructure

(b) Ad-Hoc

Figure 3: IEEE 802.11

single or multiple hopping technic. Now a suitable routing algorithm must be implemented, so the process of transmitting data will be more effective. The figure 2 shows, how the nodes form a transmission cloud.

A. Architecture

The wireless networks can be categorized based on their system architecture into two basically versions[1]. The one is Infrastructure (Figure 3a) and second is ad-hoc network (Figure 3b). The biggest different of them is infrastructure networks consist of access point and nodes, meanwhile the ad hoc networks are independent from access point.

In the infrastructure version, a terminal can't communicate directly with other terminals in the same cell and other cell. A access point here perform control messages. Messages are sent to the access point and then the access point distributes the messages to the desired terminal. If a terminal want to communicate with a terminal, which is located in other cell, the access point will relay the message to other access point, which has control over desired cell. The access points are normally wired connected. The problem in infrastructure, if the access point defects, all terminal in this cell can't perform any communication.

Unlike the infrastructure, the ad hoc networks have a different method to distribute messages. Given a network like figure 2. N1 want to communicate with N5. N5 is located outside N1 transmission range, so N1 must hop the message to N4-N2-N3-N5 or N2-N3-N5. Routing algorithm will decide, which route performs the best. There will be no problem if N4 leaves the network, because N1 still has a route to N5. Therefore ad hoc networks are robuster than infrastructure.

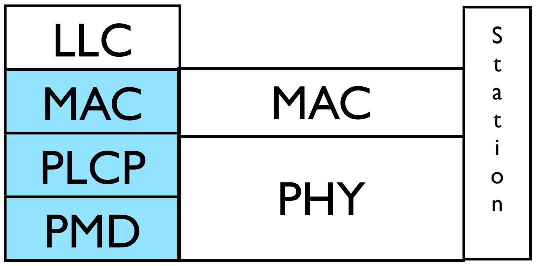


Figure 4: The Standard IEEE 802.11-protocol-architecture

1) IEEE 802.11 used for Ad Hoc Networks: The IEEE-Standard 802.11 (IEEE, 1999) describes common family of wireless LANs[1]. The standard specifies physical layer (PHY) and medium access control (MAC) of wireless transmission. The main purpose of this standard was the specification of simple and robust wireless LANs. The standard is expected to support the energy conservation of the mobile terminal, consideration of hidden terminal, and possibility of a global license-free service.

a. PHY layer: The IEEE-Standard 802.11 supports 3 versions of physical layer. The one is infrared, and two others use radio transmission to transmit data (typically in 2,4 GHz). They are Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). All of these versions provide Clear Assessment- (CCA-) signal and inform, if the medium is free. The physical layer also provide Service Access Point (SAP) with a data rate 1 or 2 Mbit/s.

The first version is infrared. The physical layer, which works with infrared light, works in a wavelength range from 850-950 nm. Infrared's arange is only about 10m. It is typically used in the room, like class, office, etc, but not outside. Because infrared can be blocked easily. Even a thin paper can block the infrared.

The figure 5 shows how FHSS works. In FHSS the available bandwidth will be partitioned into smaller bandwidthes. The sender and receiver use a narrow channel for certain time and jump to another narrow channel. FHSS is combination of TDM and FDM. There are two different Hopping, the first is slow hopping and the second is fast hopping. The slow hopping method, the sender uses one frequency for a duration time from one or more bits and the fast hopping, the sender changes frequencies while sends a single bit.

A DSSS system accomplishes directly on the data a XOR linkage with a Chipping sequence. The figure 6 show how DSSS works. Depending on procedures for the generation of the Chipping sequence, DSSS can look like coincidental noise. Therefore, this sequence is sometimes called pseudo noise sequence. The spreading factor s = tb/tc determines the bandwidth resultant signal. If the original signal needs a bandwidth w, then the spread signal possesses the range s.w.

b. MAC Layer: MAC layer is responsible for many assignment. The most important assignment is obviously control the

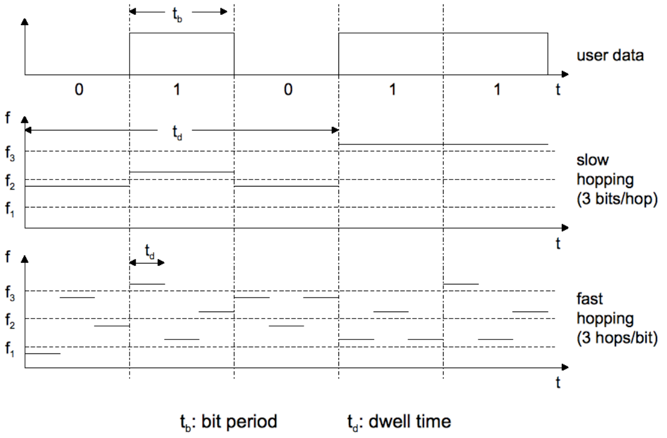


Figure 5: FHSS[2]

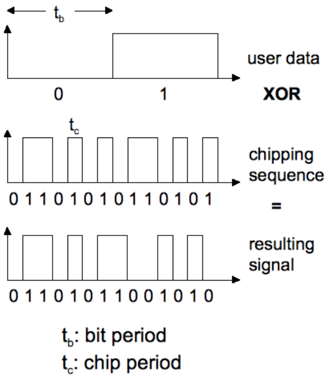


Figure 6: DSSS[2]

media access. This layer supports also roaming, authentication, and power management. The basic MAC layer's services are spoorted asynchronous data service and optional time-bounded service. The IEEE-Standard 802.11 for ad hoc provide only asynchronous data service.

There are 3 access methods described in IEEE-Standard 802.11[1]. The following are overview of these network.

1) DFWMAC with CSMA/CA
   - Every IEEE-Standard 802.11's implementation must have this method.
   - Collision avoidance via randomized "back-off" mechanism
   - Minimum distance between consecutive packets
   - ACK packet for acknowlegdements (not for broadcasts)
2) DFWMAC with RTS/CTS
   - It is optional for implementation
   - Distributed Foundation Wireless MAC
   - Avoids hidden terminal problem
3) DFWMAC with polling
   - It is optional for implementation
   - Access point polls terminals according to a list

2) Routing protocols used in Ad Hoc Networks: Routing algorithm is a real challenge issue in a wireless ad hoc network. The wireless networks like WLAN and cellular network work with supported infrastructure. Each infrastructure establishes a cell and every node in the cell can be reached by the infrastructure. So the node can send a packet to another node in the cell via infrastructure and without single- or multi-hop. If the destination node is in another cell, the infrastructure can relay to another station, in which the destination node stand. In contrast the wireless ad hoc network must work independently. A destination node can stand outside of transmission range. Therefore the networks need a routing, which can calculate a way from a sender to a receiver.

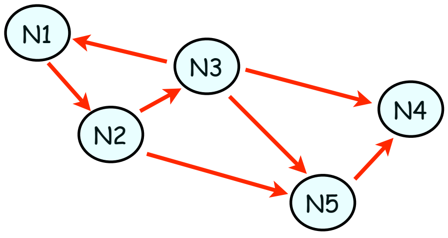


Figure 7: Asymmetric Link

The figure 7 show that the ad hoc network topology is asymmetric. Given source N1 want to send a packet to N5, the way is N1-N2-N5. N5 receive the packet and want to send an acknowledgement. Obviously N5 has information, which path N1 used. But the figure above shows, that there is no way to N1. This problem often occurs in ad hoc networks.

The simple example above show a difference between wired network and wireless ad hoc network. The following are some of routing's problem in the ad hoc networks.

1) **asymmetric link:** if a node X can hear signal from a node Y, it doesn't mean, that Y can hear signal from X too. This can happen, because X's signal is weaker, so Y can't hear signal from X. Obviously X can't direct send a packet to Y, so X must find a detour to Y. Many routing algorithms are based on symmetric connection.
2) **redundant connection:** the connection in the ad hoc networks shall be redundant to recover connection failures. A connection with high redundancy is expected to be robust though many node failures. The routing algorithm can deal with high redundancy, but it cost very much time to update the routing table.
3) **interference:** unlike wired networks, ad hoc networks don't use cable to transmit data. Transmitting data with wave is vulnerable to interferences such as, natural effect like weather, shadowing, scattering, etc. Moreover, as soon as two nodes, which are close, begin with a transmisson, they can disturb themself oppositely.
4) **dynamic topology:** the ad hoc networks' nodes can move freely (MANET). The nodes can join or leave the networks anytime. This action cause the nodes to alter their routing table.

There are different criteria for designing and classifying routing protocols for wireless ad hoc networks. For example, what routing information is exchanged; when and how routing information exchanged, when and how routes are computed etc[3].

- **Proactive and Reactive Routing**

Proactive schemes calculate the routes to various nodes in the network. So the nodes can use the route whenever they need it. Meanwhile, reactive scheme will calculate the route, if the nodes need to communicate with a destination node. The reactive schemes look like lazy schemes, because they will work, if they have to do. But the reactive schemes have smaller Route discovery overheads, because they don't have to save all possible routes in the networks. Destination Sequenced Distance Vector (DSDV) is an example of proactive scheme. Ad Hoc On Demand Distance Vector (AODV) and Dynamic Source Routing are examples of reactive scheme.

- **Single path and Multi path**
  How many paths to Node B does a Node A have? In the paragraph above, the ad hoc networks shall have redundant connection, so they can recover connection failures. Redundant connection can cause a better data throughput, but the overhead of route discovery in multi path routing is much more than that of single path routing.
- **Table driven and on demand routing**
  In the table driven routing protocols, the information from each node to every other node in the network will be often updated. A change in network topology can cause updates. In the on demand routing, the nodes don't have to update route information, since the nodes calculate the routing, if they have to communicate with other nodes.
- **Periodic and Event Driven**
  Periodical update protocols disseminate routing information periodically. Periodical updates are very useful to maintain network stability, but cause overhead. The nodes can learn about new topology and the state of the network.
- **Flat and Hierarchical Structure**
  In a flat structure, all nodes in a network are at the same level and have the same routing functionality. This structure is very suitable for small networks, but if the networks grow larger, It will no more effective. It will take a long time for routing information to arrive at destination nodes. Meanwhile, in the hierarchical structure the node are oranized into smaller partitions called clusters, and the clusters are aggregated again into larger partitions called super cluster and so on.

B. Application

Ad hoc networks are very well suited for many situations, in which a infrastructure's network can't be built or it is impossible to build an infrastucture. The interest of ad hoc networks increases rapidly in recent year, because ad hoc supports mobility and freedom in the networks. Data can be exchanged without cable, access point, or portable memory space. This section briefly explain some of applications of ad hoc networks. Nowadays computers and phones manufacturers implement ad hoc technology to their products.

a. Military use: It is perhaps regrettable that, ad hoc networks were first conceived for use in the military departement[4]. Imagine, a large number of soldiers spreads out in a large battlefield and they have to communicate each other. Installing an infrastructure in the battlefield or equip each soldier with cable is out of the question.

An alternative would be to equip each soldier in the battlefield with a transmitter, that can reach all other sodiers in the battlefield at all times. However, this methode is not suited for military use. The enemy can intercept communication easily and there would be at most one person using the channel at any given time.

Ad hoc networks are very well suited for this case. Each soldier is equipped with transmitter. However the transmitter has smaller transmission area than the transmitter from the example above, so that each soldier can only reach a few other soldiers. However, the transmitter is designed, so that they can relay messages over a hop or multiple hops. these soldiers would form an ad hoc network. This kind of network is obviously more robust, harder to intercept, and suitable to military scenario.

b. Rescue mission and emergency: Imagine, the situation after an earthquake when the communication infrastructure doesn't work anymore. A substitution of the infrastructure has be to be installed a-s-a-p to support rescue operation. It is obvious that the installed network has to be simple to configure, easy to set up and maintain, and it has to adapt to adynamic topology in order to support changes in numbers and density of participants[5].

Ad hoc networks specially MANETs can support this scenario. Ad hoc networks can be set up easily and quickly. They are designed so they are can install a network without fixed infrastructure. Ad hoc networks are temporal. As soon as a new infrastructure established in this area, the ad hoc networks can be removed easily.

c. Personal area network and bluetooth: The Idea of a personal area network (PAN) is to create a localized network populated by some network nodes that are closely associated with a single person[6]. The bluetooth technology support this scenario.

Bluetooth is a wireless local network, which has only small range area transmission (typically smaller than 10m or 100m and called piconet), operates in the unlicensed 2.4 GHz spectrum [7] and doesn't need infrastructure or cable to connect the end terminals.

A piconet is an ad hoc network, that consists of one master device and several active slave devices. The piconets can also perform a bigger network like figure 2 described, but a master device can't act as master of two or more piconets[1].

d. Wireless sensor networks: As the term implies, Wireless Sensor Networks (WSNs) are on the intersection of three different technologies: wireless communications, sensing, and networking[4]. The WSNs consist of a large number of sensor nodes, each equipped wth a wireless transceiver. The transceiver have two main roles: The sensors use it to measure and / or sense activities. And the network is used to relay the gathered information to data sinks. Therefore, the hop-count may be high. The applications of WSNs are like monitoring animal or very dangerous area.

e. Wireless mesh networks: Wireless mesh Networks (WMNs) consist of two types of nodes: mesh clients and mesh routers [4]. Mesh routers are typically equipped with power supply, so they can't move. The main role of mesh routers is to perform a singlehop (or multihop). And mesh clients

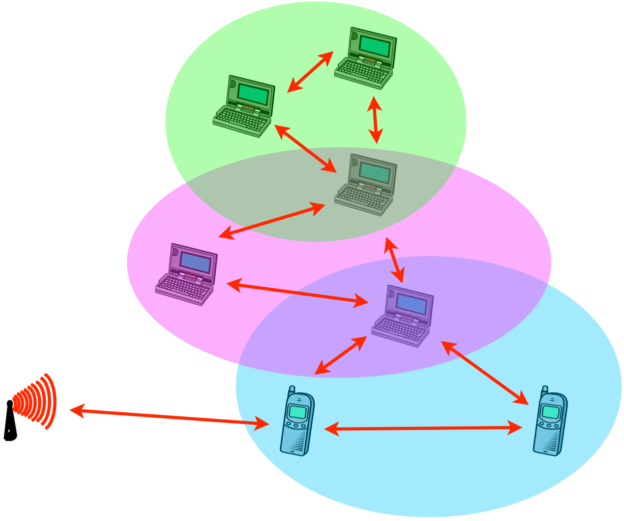


Figure 8: A Group of Piconets

are asociated with users. They can be mobile or immobile. The mesh clients are similar to mobile phone in the cellular networks GSM. Mesh clients communicate each other with via mesh routers. The applications of WMNs are like Local Area Networks (LANs) and Metropolitan Area Networks (MANs).

III. Ad Hoc Network Components

In the section 2 it was described, that the most ad hoc networks' applications are to replace infrastructure in some difficult situations. The ad hoc networks must less complicated than infrastructure. Obviously the ad hoc networks' end devices will be more complicated than the infrastructures' one. The following subsections are the important ad hoc network components.

A. Hardware

The ad hoc networks don't have any infrastructure, except they are combined with other networks' type. Only end devices are needed to establish ad hoc. Firstly the devices must be equipped with transceiver, so they can catch the incoming signal and send a signal. Secondly the devices must be implemented after the standard IEEE 802.11.

The devices like laptops, Personal Digital Assistant (PDA), smart phone are mostly implemented with the standard IEEE 802.11 so they can join a infrastructure network or ad hoc network.

B. Software

The most important software components of the ad hoc networks is routing algorithm. The following are some of most famous routing algorithms.

- **Destination-Sequenced Distance-Vector (DSDV)**
  DSDV routing is a table-driven routing scheme for ad hoc mobile networks and an Expansion of Distance Vector Routing for ad hoc networks[8]. DSDV is using a routing method distance vector, which is based on Distributed Bellman-Ford algorithm. In the networks with dynamic topology this routing protocol act very bad. This protocol has count-to-infinity problem. To gather information about the actual topology, the nodes have to swap their routing table continously. In DSDV the routing table consists of:
  - the destination's node address
  - the number of hops required to reach destination
  - the sequence number (or timestamp) of the information received regarding that destination, as originally stamped by the destination.

  The routing table can consist an entry with the same destination but it has different timestamp or number of hops. In this case the entry with newer timestamp will be chose, otherwise fewer number of hops.
- **Dynamic Source Routing (DSR)**
  This protocol performs a route on-demand when a transmitting computer requests one. DSR take two steps to do a route[9]:
  - **find the path:** A node try to find its destination, if there is at the moment no known path to the destination.
  - **maintain the path:** The obtained path muss be maintained. If a node has a problem, which is located in the path, the sender must find new path.

  Imagine a scenario from figure 7. N1 want to send data to N5, DSR take the the steps:
  - N1 sends a broadcast ((N1), id = 42, Destination = N5). Only N2 can receive the broadcast.
  - N2 hops the received message ((N1, N2), id = 42, Destination = N5), N3 and N5 can receive the message.
  - The message has reached the destination with path (N1, N2, N5).
  - But N3 still broadcasts the message to N4 and N5. Both messages will reach N5, but they will be deleted, since the path (N1, N2, N5) is shorter.

  This DSR may face problem, since the topology is asymmetric. In this scenario N5 won't be able to send back a message to N1. If N5 can broadcast to N3, the path to N1 will be (N5, N3, N1).
- **Ad Hoc On-Demand Distance-Vector (AODV)**
  AODV is similiar to DSR in that it forms a route on-demand when a transmitting computer requests one. AODV is also similiar to DSDV, it use destination sequence number to avoid loop.
  Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. These messages are received via UDP and normal IP header processing applies [10]. When a node have to perform a route. It will broadcast RREQ until reach the destination. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request.
- **Cluster Based Networks**

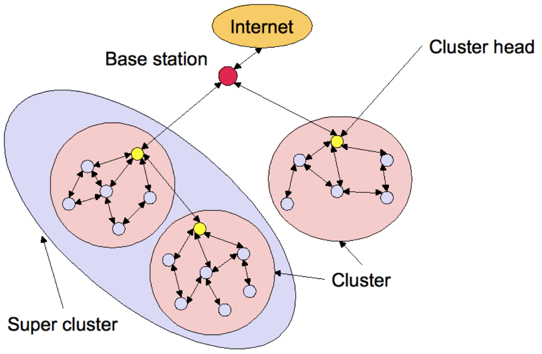


Figure 9: Clustering of ad-hoc networks[11]

Both Routing algorithms, DSDV, DSR, AODV are used only in the networks with small number of nodes and high mobility affect routing's performance. For the networks with a big number of nodes, the nodes can be formed in smaller group like figure 9.

The goal of grouping is to reduce total updates caused by dynamic topology. Let say, there are 3 smaller group in a network, group A, B, and C. Each group contains n members (eq : a1, a2, ..., an). Given that b2 leaves the entire networks and 5 seconds later a node join group C. If this network doesn't use clustering, the entire members of this network must update their routing twices. In the clustering only group B and C must update their routing. Group A want only know, that group B and C are reachable.

IV. Goal of Using Ad Hoc / Mobile Ad Hoc Networks

One of the original motivations for MANET is found in the military need for battlefield survivability[6]. In the battlefield the soldiers (with or without their warfare) have to move freely without any of the restrictions imposed by wired communications devices. They still need communication device, so they can report their position, gathered information, and communicate with other soldiers. For this purpose they can't rely on an infrastructure. In some regions, such as the desert, the jungle, or mountain there is no torrential communications infrastructure. Therefore they have to establish networks without infrastructure and ad hoc networks specially MANETs support this case.

The interest of MANETs increases rapidly in recent year, because ad hoc supports mobility and higher self organizing in the networks. The commercial applications have already implement MANETs' concept to some device, such as PDA, mobile phone, laptop, etc. Another application is to help improving education in developing countries. The children's machine "one laptop per child" program. The laptops use the standard IEEE 802.11 to establish their own communications network.

V. Advantages of Ad Hoc Networks

There are many reasons better to use ad hoc than infrastructure. The biggest ad hoc's strength is its independency from any infrastructure. Therefore, it is possible to establish an ad hoc network in any difficult situations. The following are the advantages of ad hoc networks.

a. No infrastructure and lower cost: There are situations, with which a user of a communication system cannot rely on an infrastructure[1]. Using a service from a infrastructure can be expensive for specific applications.

In an area with very low density, like desert, mountain, or isolated area it is not impossible to establish an Infrastructure. But if we compare how often the people there are using service of infrastructure and how many data per day transmitted with cost of installation, maintenance, and repair, it is maybe too expensive.

Almost the same problem with military network. It is obviously very useless to build an infrastructure in a battlefield. Aside from cost of installation, the enemy can destroy the infrastructure in short time. A independent from infrastructure network is needed for both cases.

b. Mobility (MANET only): In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users[12]. The most popular examples include military networks, emergency / rescue operations, disaster effort. In these scenarios we can't rely on centralized connectivity. MANETs support nodes' mobility. We can still communicate with our mobile devices as long as the destination is reachable.

c. Decentralized and robust: Another advantage of ad hoc networks is that they are inherently very robust[4]. Imagine that for some reason one of the base stations is not working. In this case, all users of that base station will lose connectivity to other networks.

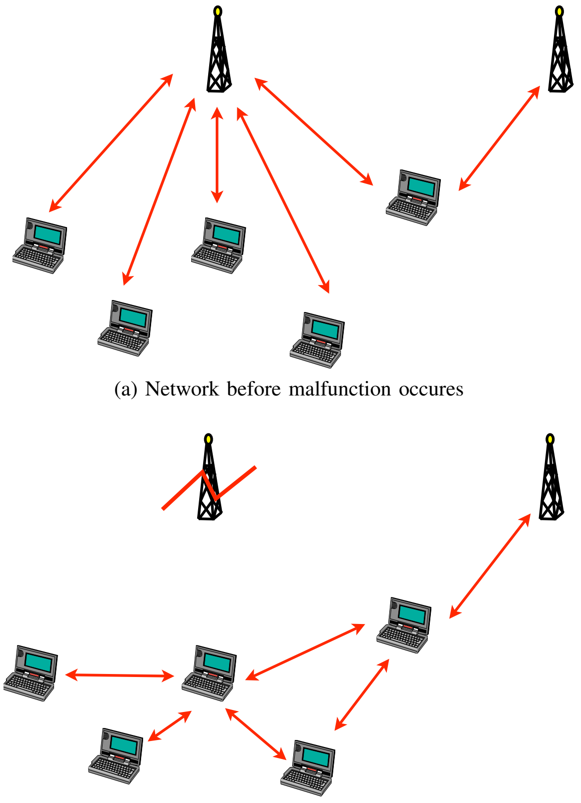
In the ad hoc networks you can avoid such problem. If one node leaves the network or is not working, you can still have connectivity to other nodes and maybe you can use these nodes to multi-hop your message to the destination nodes, as long as there is at least one way to desired node.

d. Easy to build and spontaneous infrastructure: Malfunction of a network infrastructure is sometimes not avoidable. It is obviously difficult to repair or replace the malfunction infrastructure in short time, while the network's existence must be maintained all-time. Establishing an ad hoc is a good deal in such situation. The network participants can act as ad hoc nodes and hop the messages.

VI. Disadvantages of Ad Hoc Networks

The wireless communication is very famous nowadays, using wireless can make rooms look better, because fewer cables are used. The weakness of wireless link impact ad hoc. Lower data rate, security, and medium access control are common problems in the wireless communications. Ad hocs strengths cause also some problems. The following are the disadvanteges of ad hoc networks.

a. Higher error rate: Unlike wired transmission, the wireless transmission may deal with problem the characteristic of the electronic wave. In a free room without obstacle the electronic wave propagate linear indepently from its frequency[1]. There is seldom such a situation. The obstacle causes shadowing, reflection, scattering, fading, refraction, diffraction of



(a) Network before malfunction occures

(b) Using ad hoc after a malfunction occured

Figure 10: Scenario in which ad hoc network can replace infrastructure

the wave. These propagation may lead to transmitted packets being garbled and thus received in error.

b. Lower data rate: One of biggest Problem of ad hoc networks is reduced data rates. The characteristic of wave, which is used for wireless communication, prevents wireless communication to transmit data better than wired communication. A higher frequency can transmit more data, but then it is more vulnerable to interference and performs well in short range.

c. Dynamic topology and scalability: Because ad hoc networks do not allow the same kinds of aggregation techniques that are available to standard Internet routing protocols, they are vulnerable to scalability problem[6].

Since the MANET's nodes are mobile, the routing changes as the nodes move. Current connectivity Information must to be propagated to all network's participant. Control messages have to sent around the network frequently. The increased number of control messages burdens the available bandwidth. Therefore, the ad hoc protocols are typically designed to reduce the number of control messages, such as by keeping the current information.

A good algorithm for ad hoc networks must be able to evaluate and compare networks' relative scalability in the face of increased number of nodes and nodes mobility. It is very important to know how many control message is required. So we can control bandwidth's usage.

d. Security: Due to dynamic distributed infrastructure-less nature and lack of centralized monitoring points, the ad hoc networks are vulnerable to various kinds of attacks[13]. Unlike wired channel, the wireless channel is accessible to both legitimate network users and malicious attacker. Therefore, the ad hoc networks are susceptible to attacks ranging from passive attacks such as eavesdropping to active attack such as interfering[14]. Especially for MANET, limited power consumption and computation capabilities, due to energy limitation, causes incapability to execute computation-heavy algorithms like public key algorithms.

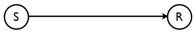
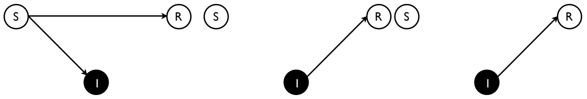


Figure 11: Normal Data Flow



(a) Eavesdropping (b) Modifying (c) Masquerading

Figure 12: Security Attacks

Passive attack means, that the attacker does not send any message. The attacker just listens the channel, therefore, it is almost impossible to detect this attack. In contrast, the active attacks modifies, deletes the packets, injects packets to invalid destination. Active attack can be detected.

There are numerous security problem issues in the ad hoc networks. The following are some of the security problem of IEEE 802.11.

1) **Eavesdropping** (passive), a non-legitimate listening into a transmission between two nodes.
2) **Traffic analysis** (passive), the attacker monitoring the transmission for patterns of communication.
3) **Masquerading** (active), the attacker pretends to authorized user of a system in order to gain access to it or to gain access to it or to gain greater privileges than they are authorized for.
4) **Replay** (active), the attacker spies transmissions and retransmits message as the legitimate user
5) **Message modification** (active), the attacker alters a original message by deleting, adding to, modifying it.
6) **Denial-of-service or interruption** (active), the attacker prevents or prohibits the normal use or management of communications facilities.

e. Energy limitation (MANET only): A MANET network allows mobile nodes to communicate in the absence of a fixed infrastructure. Therefore, they operate with on battery power. Because of these limitation, they must have algorithms which are energy-efficient as well as operating with limited processing and memory resources[15]. The usage of available bandwidth will be limited because nodes may not be able to sacrifice the energy consumed by operating at full link speed.

It is also very annoying, while receiving data from someone with PDA, the battery is almost depleted. Repeating the transfer process after recharging is necessary. Therefore a MANET is not suitable for a permanent network.

VII. Comparison

There are some keys used in this section to compare the ad hoc networks and infrastructure networks. The ad hoc networks described above have show great features but not perfect. The following are the keys used to compare ad hoc and infrastructure:

- **Infrastructure:** An infrastructure is built to control the end terminals. All message will be sent to it and it will broadcast the messages to the destination node. In absence of infrastructure the end terminals lose their connection.
- **Mobility:** This key refers how the end terminals can move. They can move freely or restricted. Perhaps the mobility can also affect network's performance too.
- **Scalability:** Scalability in the wireless networks describes the performance of the networks in the faced of increased number of nodes and nodes mobility.
- **Routing:** Routing is the process of selecting paths in a network. The selection of routing algorithms is very decisive, since a routing algorithm is dedicated only for specified purposes.
- **Security:** Both infrastructure and ad hoc must deal with wireless security problem. There are some differences between ad hoc and infrastructure, which are described below it.

	Advantages	Disadvantages
Infrastructure	As described in the previous sections the ad hoc networks don't rely on any infrastructure. They work independently, are more robust, and it is cheaper to form a ad hoc network. There is no installation, maintenance cost.	Without any help from infrastructure, the nodes have to work harder. They have to hop the messages, secure their own resource from attackers, perform a routing table, etc.
Mobility	Unlike the infrastructure networks, in which node's moving is restricted by cell's border, in the ad hoc networks, a node can theoritical move freely. As long as this node can hop to a node inside the network, it can also communicate with other node in this network.	In the practical, it is hard to form a network, in which a node can move freely.
Scalability		Depent on routing algorithm, how the ad hoc networks can perform well. In a network with a large number of nodes and high mobility a table driven algorithm won't perfrom well, because there will be big overhead. Generally the infrastructure networks perform better in this situation. The infrastructure networks have only specify tasks, so they can handle more nodes.
Routing	Given a network topology like figure 7. If N3 or N5 doesn't work anymore or leaves the network. N1 still can communicate with N4. In the infrastructure networks, if the access point is defect, there will be no more communication in the affected cell.	Mobility and increased or decreased number of nodes can force some routing algorithms to alter their routing table.
Security	Some attacks can cause malfunction. If one of participant is attacked and it doesn't work anymore, The network can relay the messages through other route (if alternativ route is available).	Internal attacks may be possible via ad hoc transmissions[14]. It means, the attacker can disguise itself as a ad hoc participant. It can spy, modify, or delete the hopped messages.

Table I: Advantages and disadvantages of ad hoc network

VIII. Conclusion

Mobility in the wireless networks is very popular nowadays. Many peoples in the street walk and are using small devices like PDA, laptops, or phone to communicate, listening a music, write SMS, exchanging data with other people near them, etc.

The wireless infrastructure networks support great mobility and very popular among the folks. But this kind of networks are centralized, not flexible, and sometimes too expensive. If a infrastructure is defect, the cell established by this infrastructure will be gone too. The nodes in this cell can't communicate again.

The presence of ad hoc networks covers the infrastructure's weakness. Since the ad hoc networks are independent from infrastructure, the nodes must be able to work together to establish a greater network. They have multi hop the packet, if they have to send a packet to a destination nodes outside their transmission range.

Therefore, routing algorithms are the main challenge. Since the nodes are mobile, link between nodes are not symmetric, and the topology are always changed, the routing algorithms used in wired network must be modified or must be invented.

The ad hoc networks still have to deal with wireless problems, such as security and higher error rate. Specially MANETs have to consider their power supply, since they are not supported with fixed power supply.

At least, the ad hoc networks are developed not to replace the infrastructure networks. With the great number of wireless user and frequency limitations, it is unlikely possible to control independent network. The ad hoc networks can replace the infrastructure networks only for a short time and are used for some specific situation, in which the infrastructure networks fail. A combination of both networks like figure 13 can offer great output, like connection between ad hoc and Internet.

References

[1] J. Schiller, *Mobilkommunikation*. Addison-Wesley Verlag, 2000.

[2] J. Schiller, "Wireless transmission," 2008.

[3] K. U. R. Khan, R. U. Zaman, and A. V. Reddy, "Performance comparison of on-demand and table driven ad hoc routing protocols using nctuns," pp. 336–341, 2008.

[4] S. Toumpis and D. Toumpakaris, "Wireless ad hoc networks and related topologies: applications and research challenges," *e & i Elektrotechnik und Informationstechnik*, vol. Volume 123, pp. 232–241, 2006.

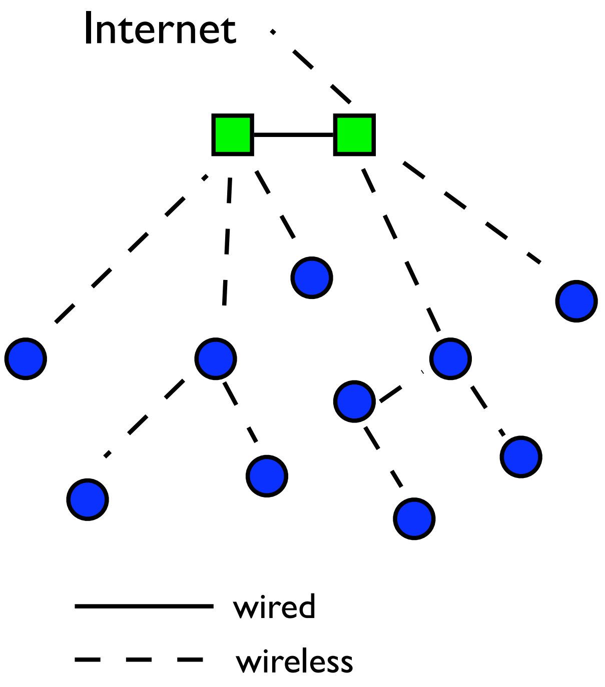


Figure 13: combination of infrastructure and ad hoc

[5] M. Günes, B. Blywis, and F. Juraschek, “Concept and design of the hybrid distributed embedded systems testbed,” August 2008.

[6] Perkins and C. E., *Ad hoc networking*. Addison-Wesley Verlag, 2001.

[7] “The official bluetooth.”

[8] C. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers,” 1994.

[9] D. Johnson, Y. Hu, and D. Maltz, “The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4,” *Network Working Group Request for Comments: 4728*, 2007.

[10] C. Perkins and E. Belding-Royer, “Ad hoc on-demand distance vector (aodv) routing,” *Network Working Group Request for Comments: 3561*, 2003.

[11] J. Schiller, “Network protocols / mobile ip,” 2008.

[12] “National institute of standards and technology: http://www.antd.nist.gov/index.shtml.”

[13] D. Wang, M. Hu, and H. Zhi, “A survey of secure routing in ad hoc networks,” *The Ninth International Conference on Web-Age Information*, pp. 482–486, 2008.

[14] T. Karygiannis and L. Owens, “Wireless network security 802.11, bluetooth and handheld devices,” 2002.

[15] S. Mueller, R. P. Tsang, and D. Ghosal, “Multipath routing in mobile ad hoc networks: Issues and challenges,” *Performance Tools and Applications to Networked Systems*, pp. 209–234, 2004.