# Ad hoc networks:
# Overview, applications and routing issues

Kristoffer Karlsson IT3
Billy Ho IT3
Chalmers University of Technology
kriskarl@student.chalmers.se, billy@student.chalmers.se

**Abstract**
This paper intends to give an introduction to ad hoc networks in general. The following topics will be discussed: The definition of ad hoc networks and its applications, moreover the paper dives a bit deeper into how routing is handled in ad hoc networks and describes a couple of different routing methods. The paper discusses routing methods from two different perspectives position based and adaptive in each of these two categories it describes a couple of different methods in more detail. Finally the paper briefly discusses security issues related to routing protocols this is intended to give the reader a glance of which security issues arises in the design of ad hoc networks.

**Keywords**: Ad hoc networks, Ad hoc network routing, Ad hoc network applications, Adaptive routing, Position based routing, Ad hoc routing protocol attacks.

## 1. Introduction

The rapid growth of Internet has made communication an integrated and highly important factor of computing. In today's society with the development of mobile devices it has become important to stay online all the time. In order to stay online all the time it must be possible to set up a network fast and cost effective when moving between different infrastructures, ad hoc networks deals with this kinds of issues.

Furthermore in military operations or after environment disaster it is important to establish communication fast in addition it is highly probable the existing infrastructure has been destroyed. After the ad hoc network has been established the nodes that connect the network might move, say for example that one military squad is under heavy attack and has to escape. In ad hoc networks nodes should be able to move freely and the information should be routed through new paths after old ones have been broken, the network should also be able to handled clustering. The advent of ad hoc network has given birth to new kinds of routing algorithms and new security threats.

More complications arise in ad hoc wireless networks because the components usually have much lower capacity than their wired counterparts, this gives makes congestion and overload common rather than an exception which it is in wired networks. Due to the fact that ad hoc networks should be possible to establish in tough context, factors such as noise and disturbance play a major role in the design.

## 2. Definition

Ad hoc is defined as "Arranged or happening when necessary and not planned in advanced" according to oxfords advanced learners dictionary. This gives an explanation of what ad hoc networks are is to say networks set up on the fly for a special purpose. Furthermore ad hoc networks are usually such networks that are set up for one time occurrences such as conferences or military operations. This can be paraphrased into the following definition an ad hoc network is a flexible and adaptive network with no fixed infrastructure.

## 3. Applications

Ad hoc network has many applications two of them are already mentioned is to say crisis management and military operations. Another application is Bluetooth which is designed for personal use and enables printers, scanners, mobile phones and music players to be connected wireless to a personal area network this creates a tremendous flexibility because it enables devices to move freely between different networks. Ad hoc networks can also be used in the multi player game, one can imagine a game played from a device that can establish communication with other nearby devices, and these devices can then establish a cluster of interconnected devices and use this as a platform for playing the game. There are many implementations of ad hoc networks one of them is today's laptops equipped with 802.11 wireless PCI cards, they establish an ad hoc network, if the ad hoc mode is activated. This is especially useful for business meetings in places where no current infrastructure is available say for example on an ad hoc conference in for example a restaurant. If those taking part wishes to share data such as reports, diagrams and statistics they can activate their ad hoc mode and effortlessly transmit the data. This has proven extremely useful and completely eliminates the need for cable and routers.

## 4. Routing

There are many routing algorithms. Position Based Routing, Adaptive Routing and SAFAR will be discussed here. In Position Based Routing and Adaptive Routing, there are different routing approaches.

### 4.1. Position Based Routing

Here routing in which a packet is to be sent from a source node to a destination node in a given wireless network will be considered. The destination node is known and addressed by means of its location. Routing is performed by a scheme based on this information.

The distance between two neighbour nodes can be estimated on the basis of incoming signal strengths. Relative coordinates of neighbour nodes can be obtained by exchanging such information between neighbours.

Position based routing could be used in wireless local area network, packet radio networks, home and office networks and sensor networks. Especially wireless sensor networks, which will likely be widely deployed in the near future because they greatly extend our ability to monitor and control the physical environment from remote locations.

There are several classes of existing position based routing schemes. Some of the will be described.

Progress and Direction Based Methods

Given a transmitting node S, the progress of a node A is defined as the projection onto the line connecting S and the final destination of the distance between S and the receiving node. A progress is positive if the next routing step is in forward direction, otherwise the progress is negative.

Basic Distance, Progress and Direction Based Methods use these concepts to select the next routing step.

There are different ways to route packets. One way is the MFR (Most Forward within Radius) routing algorithm, in which packet is routed to the next step with the greatest progress. Another way is to use the compass routing method, called the DIR method. In this method, the source or intermediate node A uses the location information of the destination D to calculate its direction. The packet is forwarded to the next node C, such that the direction AC is closest to direction AD. This progress repeats until destination is reached.

A variant of greedy algorithm, called GEDIR, could also be used, where the message is dropped if the best choice for a current node is to return the message to the node the message came from. That indicates that a failure has occurred. Greedy routing is usually a part of other routing schemes. For instance, it is used in several location update schemes.

Partial Flooding

In directional flooding-based methods, a node A sends a message to many nodes where the direction from A to any of these nodes is closest to the direction of the destination D. In order to control the flooding, it is required that nodes can memorize past traffic and to

avoid forwarding the same message more than once. Some methods that belong to this class are DREAM and LAR.

Flooding can be partial because it is directed towards nodes in a limited sector of the network and can only be used for path discovery or for packet forwarding.

In DREAM, the message is forwarded to all neighbour nodes whose direction belongs to the selected range. DREAM uses a limited flooding of location update messages.

In LAR (location aided routing), the source or an intermediate node A will forward the message to all nodes that are closer to the destination than A.

Depth First Search Based Routing

In GRA (geographic routing algorithm), nodes are required to partially store routes towards certain destinations in the routing tables. GRA applies greedy strategies in forwarding messages. If a node S discovers that it is closer to the destination node D than any of its neighbour, it starts a route discovery protocol. The route discovery protocol tries to find a path from S to D and updates the routing tables towards D at any intermediate nodes with this information. There are two route discovery strategies, breadth first search (equivalent to flooding) and depth first search (DFS). In DFS, each node puts its name and address on the route discovery packet, and then it forwards it to a neighbour node who has not seen the packet before. If a node can not forward the packet, it removes its name and address from the packet and returns the packet to the node that forwarded to this node. Each node accepts a given packet only once in the forward mode (also accepts the same packet if returned to it).

Hierarchical Routing

One of the main strategies used to combine nodes location and hierarchical network structures are the Zone Based Routing. In Zone Based Routing, nodes within a zone update their location between themselves regularly and apply the shortest path routes between them. Each node records the location of each zone, by treating each zone as a destination. If a message is not sent to a destination within the same zone, the sender will send route requests to each of the zone. The zone that contains the destination replies with exact coordinates of the destination back to the sender node. The sender node then learns the path to the destination and sends the full message towards the destination.

Assisted Routing

In Assisted Routing, a node can count on the assistance of some other nodes called friends, i.e. some nodes help other nodes in performing their routing tasks. The network is represented as a large graph, where edges correspond to the ”friend relationship”. A node S is a friend of node T if T thinks that it has a good path to node S and T decides to keep S in its “friend list”. The resulting graph is highly clustered with a number of shortcuts. When a node is selected for being a collaborative node, the shortcuts are

effective for the routing tasks, and in particular for selecting paths. When a source node S wants to find a path to destination node D, it requests assistance from some friend node. If the friend is in condition to collaborate, it tries to provide node S with some path to D (with or without collaboration of its own friends, depending on it already has the path or not).

### 4.2. Adaptive Routing

On-demand routing is important for mobile devices to communicate in a wireless network. Since devices in an ad hoc network joins and leaves the network at will and in a totally asynchronous manner. Thus, it is important that a wireless network can provide ”anytime anywhere” computation due to its robustness and inherent fault-tolerance.

There are two major classes of ad hoc routing protocols, reactive on-demand and proactive table-based. Proactive table-based protocols are inefficient in the sense that it requires periodic update of the routing information stored in the routing tables, even when there is no data traffic. One advantage with proactive table-based protocols, compared to reactive on-demand protocols, is that the set up delay for a data transfer is expected to be shorter because a route is already stored in the table for use. But however, the route stored in the table may no longer exist or have become unusable when the actual data transfer is to be taken place. It could be due to the mobility of the mobile device in the network, i.e. its geographical locations may have been changed when a data transfer is required, meaning that a previously set up route useless. Another reason could be that the quality of the channels among the mobile devices is inevitably time-varying making the links in a route no longer useable, even though the geographical locations do not changed much.

State-of-the-Art Protocols

ABR (Associativity Based Routing) is a source-initiated on-demand routing protocol. A mobile device does not need to keep a route to every other device. ABR is different from other protocols in the sense that the route is not chosen with shortest-path, but on a long-lived basis. This makes the route more robust (not easy to break due to mobility) and the maintenance of route will become easier (number of route reconstruct messages is reduced, which means that the routing overhead is reduced and more bandwidth is saved). The essence of ABR is that as a mobile device moves, its associativity with the neighbour devices also changes. In ABR, each mobile device periodically transmits ”hello messages” to other devices to signify its existence. When these ”hello messages” are received by its neighbour devices, it causes the associativity to increase between the sending and receiving devices. The greater the the associativity is, the more stable of this device will be. Note that a high associativity of the device means a low mobility of the device.

AODV (Ad-hoc On-Demand Distance Vector) is a reactive on-demand protocol. In this protocol, each device does not need know a route to every other device. It does not need to periodically exchange route information with neighbour devices. Only when a mobile device has packets to send to a destination does it need to discover and maintain a route to that destination device. In AODV, each device has a route table for a destination. The route table stores destination address, sequence number, active neighbours, and expiration time for the table. Expiration time is updated each time the route is used. If the route has not been used for a specified period of time, it will be discarded.

Link State Routing protocol was originally designed for wireline networks. In this protocol, each mobile device has its own view of the network. When a mobile device wants to forward a packet, it uses the shortest-path algorithm to find the next hop to forward the packet to its destination. Thus, each mobile device must keep an up-to-date view of the network. When a mobile device finds that a link cost has changed with one of its neighbour devices, it will flood this change throughout the whole network. Thus, all other mobile devices will eventually update its view of the network.

In DSDV (Destination Sequenced Distance Vector) routing protocol, each device maintains a routing table containing entries for all the devices in the network. In order to keep the routing table completely updated at all time, each device periodically broadcasts routing message to its neighbour devices. When a neighbour device receives the broadcasted routing message and knows the current link cost to the device, it compares this value and the corresponding value stored in its routing table. If changes were found, it updates the value and recomputes the distance of the route which includes this link in the routing table.

Receiver Initiated Channel-Adaptive (RICA) Routing

The RICA protocol is a reactive on-demand algorithm. A source mobile device does not permanently keep a route to any destination. The source device will try to determine a route only when it has packets to send to a particular destination. When a source device wants to transmit a packet, it first generates a route request (RREQ) packet. It then broadcast the RREQ to all devices within transmission range. Neighbour devices will forward the RREQ to other farther devices. This goes on until the RREQ reaches the destination device. The destination device then generates a route reply (RREP) and unicasts it along the selected route back to the source device (the selected route can be computed from RREQ, where a fields holds a list of all intermediate devices).

### 4.3. SAFAR

SAFAR is a mobile wireless routing protocol for ad hoc networks it combines both proactive and reactive routing described above. Due to the fact that most wireless devices has lower capacity than wired it takes a new approach to routing and strives to maximize the usage of bandwidth at every stage. The protocol uses a so called fitness-based routing table which is that it takes into consideration when routing how fit is to say how good a

node is to route information through. The fitness of a node is dynamic hence it can change over time.
SAFAR is built on the following assumption

1. Every node has its own fitness information
2. All links are symmetric

The protocol is based on the fact that nodes with low bandwidth should not have to handle the overhead needed to maintain a path, thus the low bandwidth nodes use a reactive approach. On the other hand the nodes with high bandwidth use a proactive approach they send data between each other necessary to build a path. The fitness of a node determines how many nodes it can maintain contact with. This architecture enables the high bandwidth node to take care of most of the communication and thus maximizes the bandwidth of the system and does not make the low bandwidth nodes overloaded. This method is called hybrid because is uses both proactive and reactive.
When routing packets SAFAR takes a two-stage approach in the first stage the protocol tries to send the packet through the existing infrastructure which has been established proactively, unless must nodes have very low fitness factor this will probably work if the nodes are in the same area. If the first stage fails the protocol will enter the second stage which here the protocol uses an approach similar to the on-demand approach describe above. [2]

**5. Attacks on routing protocols**

The types of attacks can roughly be divided into two types, passive attack and active attacks. In the former the attacker does not strive to bring the network down instead the attacker eavesdrops and gathers information. This information can later be used to launch an attack, this type of attack is called active attack and it could be launched on a weak node on the ad hoc network, this attack could be everything from a denial of service attack to a masquerade attack. One of the hardest attack to defend against is the denial of service attack this might make an ad hoc network vulnerable if it depends on a single link for routing information between two clusters. Although in general ad hoc networks are fairly protected against denial of service attacks because they dynamically establishes new paths if a node has been taken down.
Besides from denial of service attacks there are other types of attacks which pose a threat to routing protocols. One of them is attack by dropping packet, which is when a malicious node on the network deliberately drops packets. This attack can be divided into two types one is when the malicious node drops all packets, this is called black holes. The other is when it is selective about which packets it drops this is called grey holes. This attack is extremely hard to defend against because it is very difficult to detect.
Another dangerous active attack is the modification of control packet fields attack. This attack alters the control packet fields this can be extremely dangerous because if an attack like this is carried out properly it will create a gap between the network's current state and how the nodes perceive the state of the network. One example of such attack is to modify the route sequences number, this attack idea is for a malicious node to advertise this it has the shortest path to the node of which packets it wants the intercept packets. So all node sent to that node will go through the malicious node thus it can read them.[3]

## 6. Conclusions

The fast pace of which mobile technology evolves will probably result in new demands. Many of those demands will probably be satisfied by the development of robust, effective and cheap ad hoc networks. These new technologies will make it possible to establish robust network on demand and no further equipment will be needed. Ad hoc technologies will also prove useful in situations where the infrastructure has been destroyed. It may save life if a crisis management group fast can establish communication links and communicate with the outside world. Unfortunately developing effective ad hoc networks is not an easy task, the routing algorithms are subject to new problems which must be solved. As always then computers communicate over an open medium it can be subject to attacks many attacks are harder to defend against due to the dynamic structure of ad hoc networks.

## 7. References

[1] Xiuzhen Cheng, Xiao Huang, Ad hoc wireless networking, Springer; 1 edition (December 31, 2003)

[2] Jigar Doshi and Prahlad Kilambi, SAFAR: An Adaptive Bandwidth-Efficient Routing Protocol for Mobile Ad Hoc Networks, Sri Venkateswara College of Engineering

[3] Siddhartha Gupte, Mukesh Singhal. Secure routing in mobile wireless ad hoc networks, Department of Computer Science, University of Kentucky, Lexington, KY 40508, USA