Routing in ad-hoc networks
Marina Dupcinov, Srdjan Krco
Applied Research Lab, EEI, Ericsson Ireland

I Introduction
Ad-hoc networks are formed by users or devices wishing to communicate, without the necessity for the help or existence of any infrastructure or centralised administration. Each node in an ad-hoc network has a wireless access interface (Bluetooth, WLAN, UWB, etc.) and is free to join 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. Applications of ad-hoc communication include commercial and educational use, emergency cases, military communication, sensor networks, etc.

Ad-hoc networks may comprise various devices, all of which have the following constraints in common:
- Limited bandwidth - hundreds kbits/s to few Mbits/s;
- Limited power supply - battery driven devices;
- Limited transmitter range – few hundred meters.

Due to the limited range of wireless interfaces, multiple hops may be needed for communication. As nodes in the network can move freely and randomly, frequent topology changes occur and routing protocol has to be able to handle such changes efficiently.

Wireless nodes are also very susceptible to various interferences that can lead to sporadic connectivity patterns, causing useless routes to be established, accompanied with low throughput and other problems.

As the most devices in ad-hoc networks are battery driven, power consumption is another important issue since wireless transmission is the main power consumer in an ad-hoc node. The current routing protocols, however, do not take care of node’s power resources, but always send packets using the maximum transmit power, although the required energy for a successful transmission decreases rapidly with decrease of distance, typically with fourth order of magnitude.

The next section gives an overview of the existing routing protocols for ad-hoc networks. In section III, the AODV routing protocol principles are given and the section IV describes some of the issues observed during implementation and testing of this protocol. Section V presents some of the results obtained from testing live, WLAN 802.11b based, ad-hoc network. Section VI concludes the paper.

II Ad-hoc Routing Protocols Overview
There are number of proposed protocols for IP based ad-hoc mobile wireless networks [1]. Although developed for the same type of network, these protocols adopted variety of approaches. They can be divided into the following groups:
(a) Table-driven
(b) Source-initiated on-demand driven and
(c) Location based.

Table-driven routing protocols maintain the routing information from each node to every other node in the network, regardless of whether the route is ever used. To store all the necessary information, one or more tables are being maintained by each node. If a change in the network topology occurs, the updates about the change are propagated throughout the network. There are obvious disadvantages of this approach: the bandwidth, which is a scarce resource in ad-hoc networks, is not efficiently used; also, the excessive control traffic consumes the power, which is also the problem with battery driven devices. On the other hand, since the route to each destination is always available, there will be no delays in traffic handling which is necessary for real-time traffic.

Source-initiated on-demand routing strategy (frequently referred to as reactive routing) was developed exclusively for ad-hoc networks. These protocols do not maintain permanent routing tables. Instead, routes are discovered only when source node needs them. Source node initiates the route discovery procedure. When the route is found, it is being maintained as long as it is used or until the destination becomes unreachable. The disadvantage is the latency that route discovery might produce. In small networks this is usually not the problem, but in networks with great number of nodes it can be a serious limitation, especially for real-time traffic.

With GPS becoming commercially available to broader population, a new approach to routing appeared. Location based protocols, which utilise location information, were proposed. In order to limit flooding of the network, the estimated location information, based on the last known position, direction and speed is being used to limit the area which is flooded with control messages. Also, the criterion for choosing the best next hop in the route to destination, based on location information, is proposed: the nodes that are in the direction from source to destination are the best candidates to become the next hop to the particular destination.

There is no single routing strategy, which is the best in all situations. Depending on different scenarios (mobility, size of the network or traffic patterns) and applications used, various protocols may prove to have more or less advantages/disadvantages. Hybrid ad-hoc routing protocols are proposed as well [2], which toggle between table-driven and on-demand approaches.
There are several routing protocols proposed in the MANET working group [1]. However, three of them, AODV, DSR and OLSR [3], seemed to gain the most interest in the research community and were most frequently simulated. In order to evaluate the performance of an real ad-hoc network, we have implemented the AODV (Ad-hoc On-Demand Distance Vector) routing protocol.

III Overview of AODV routing protocol
AODV [2] routing protocol is a reactive protocol based on the classical Bellman-Ford routing mechanism. It provides unicast, multicast and broadcast communication. The route discovery is initiated only when a route is needed. It is based on a query/response model. Once discovered, active routes are maintained as long as the source node is using them. When they are not used, the routes expire, and after a delete period they are completely removed from the routing table. Only a single route can exist between any source-destination pair. The AODV guarantees establishment of loop-free routes. For that purpose, each node maintains its own sequence number. The sequence number is incremented each time a node is involved in creating a new route, whether it is the source node looking for the new route for a particular destination, destination itself or an intermediate node offering a route to the requested destination. A set of predecessor nodes is maintained per routing table entry. Predecessor nodes are neighbouring nodes that use this entry while routing the packets.

Route Discovery
The route discovery procedure is invoked when the source node needs a route to a destination. It broadcasts the Route Request (RREQ) message and sets a timer to wait for a response. When a node receives the RREQ, it first updates or creates a reverse route entry for the source in its routing table. This route may be used to propagate eventual Route Reply (RREP) message back to the source. Next, it checks whether one of the following conditions is met: the node is the destination itself or it has a valid route to the destination with associated sequence number greater or equal to that contained in the RREQ. If neither of these conditions is met, the node rebroadcasts the RREQ. If the node meets one of the conditions, it unicasts the RREP back to the source via the previously created reverse route. When an intermediate node receives the RREP message, it creates the forward route entry for the destination node in its routing table. Then, it forwards the RREP to the source. When the source node receives the RREP, the route is established and the source can start using it. If other RREP messages are received with either (a) greater destination sequence number or (b) equal destination sequence number, but smaller number of hops, the routing table is updated with new information.

IV Observed issues
At the initial stage of implementation, we have noticed several issues with different “ad-hoc” modes supported by different WLAN cards vendors [4]. The initial testing of the implementation has shown additional issues with the ad-hoc mode, which are probably due to different interpretations of the 802.11b specification. These issues are described in the following paragraphs.
In one scenario, a 2-hop route was established between nodes A and C via node B. After route establishment, node B started to move towards the node C (away from node A) and at certain point user traffic throughput almost ceased completely although routing tables did not change and the A-C route was valid (Hello messages were exchanged between nodes regularly and data was sent from node A). This was a peculiar behaviour and we have performed some additional testing in order to determine the cause of it. The outcome of this testing was that broadcast and unicast packets are not transmitted using the same bit rate: unicast rate was 11Mbit/s, while broadcast rate was 2Mbit/s. Due to this, different coding schemes are used and more energy per bit is available to broadcast packet which effectively means that broadcast packet have larger range than unicast packets. The difference in ranges has a detrimental effect on the neighbourhood detection and hence on the performance of every routing protocol that uses similar technique to discover neighbours as AODV.

We proposed a solution to this problem based on differentiation of neighbours to “good” and “bad” neighbours, based on the link quality. “Good”-“bad” status is determined dynamically and packets are received only from “good” neighbours. The work on the above problem has also shown that using number of hops as the only metric is not a very good solution. Due to various interferences and degradations of links, there are scenarios where the route quality would be much better if more good-quality hops than less poor-quality hops were used.

Another issue is related to usage of MAC layer acknowledgments. We have analysed the possibility of using these acknowledgements for neighbourhood detection, as proposed by the AODV draft. Before we were able to get any information from the MAC layer, the WLAN card driver had to be modified. The implemented modification allowed us to gather SNR value for each received packet and info whether a packet sent to that particular MAC address was acknowledged or not. This puts substantial extra workload on processor especially when there are many nodes in the neighbourhood. Moreover, an efficient way of communication between the routing protocol and the driver have to be found if this feedback is to be used.

The IEEE802.11 specification defines that each successfully transmitted packet is acknowledged on the MAC level. However, the driver delivers only negative acknowledgments without explicitly stating which packet the NACK refers to, so it is very complicated to determine when a specific Hello message was not delivered. The other way to use the NACKs could be to set a threshold for the acceptable number of NACKS on a “good” link. This approach could work when light traffic is present in the network, but, as our experiments have shown, cannot be used when the traffic load is high.

We performed throughput measurement of multi-hop connections using FTP to transfer large files. Nodes were placed in positions where a stable 3-hop connection was possible. When a light traffic (e.g. ping 10 times per second) was introduced in the network, the transmission was nearly error free. In the same configuration the burst transfer of large files was slow, because many data packets get lost (MAC-layer feedback showed in average 20-30% drop-rate) and the route gets lost too often. The main reason for loosing the route is that during the time data packets are transferred with high rates, too many packets get lost due to collision problems, including the control packets needed for the AODV protocol. In this case, then, categorising neighbours as good or bad based on MAC layer feedback can further decrease the performance of the network. This occurs because neighbours erroneously get categorised as bad, routes become broken and route re-establishments are required. Since the quality of the connection between the nodes is entirely adequate, this wastes bandwidth and results in poorer application-level performance. Collision problems would be solved using RTS/CTS but this feature was not supported in the ad-hoc mode of WLAN cards we were using (ELSA MC11).

Measurements also showed that unicast transmission failed more often than broadcast transmission, and broadcast transmissions were possible even when no unicast packets could be sent. This explained the existence of “grey” areas where one-hop routes were maintained, but the transmission was poor or not possible at all. The described problem is not related to the AODV routing protocol only, but to all routing protocols that use broadcast messages for neighbourhood detection.

V Ad-Hoc Networks Throughput

There are few theoretical studies, which tried to estimate per node capacity and throughput that can be expected in ad-hoc networks.

One would expect that capacity of wireless networks grow with the area they cover due to the fact that distant nodes can transmit concurrently. However, the very fact that nodes must act as routers and forward another nodes’ traffic has a significant impact on the end-to-end throughput available to each node.

In [5], it is concluded that end-to-end throughput available to each node in the network with n nodes under optimal conditions is:

$$O\left( \frac{1}{\sqrt{n}} \right),$$  \hspace{1cm} (1)

using a non-interference protocol.

Based on (1), if number of nodes in the network grows to infinity, available throughput per node becomes zero. The conclusion that can be drawn from these results is that in general case ad-hoc networks do not scale well. In [6], authors suggest that above analysis assume a random communication pattern, where communication between each node pair is equally likely, which may not be true for large networks. Users in large networks may tend to communicate mostly with physically close nodes. If such local communication dominates in the network, path lengths will stay nearly constant as the network grows and so will the per node throughput. The capacity of a chain of nodes is analysed. If nodes in a chain are distant enough, they won’t interfere with each
Routing in ad-hoc networks is one of the most challenging areas in ad-hoc networking. There are many routing protocols proposed specifically for this type of networks and here an overview of the existing approaches to routing is given. We implemented AODV routing protocol and tested it in an IEEE 802.11b based network. The connectivity problem related to WLAN cards was identified and a solution proposed. Some results of the experimental evaluation of the network behaviour are presented. They showed that performance of the network could vary significantly due to radio conditions and packet collisions, caused by nodes transmitting concurrently. A reasonable UDP throughput of 1 Mb/s can be obtained on 5 node linear chain networks. This is sufficient to accommodate some tens of users requiring constant bit rate of some tens of Kbs. TCP performance varies even more. In some cases a very poor behaviour was encountered, which only confirmed well known problems of TCP operating in wireless environment.

The future work will focus on interaction of ad-hoc networks with Internet.

VII References


Abstract: Ad-hoc networks comprise devices capable of organizing the network without the need for existence or help of a centralised authority. In such networks one of the main issues is establishment and maintenance of communication paths between nodes. Various routing protocols have been proposed for that purpose and this paper describes one such protocol – the AODV. Some issues observed during the implementation of the AODV are described and possible solutions are proposed. Network performance results obtained during tests. This can be attributed to the radio environment – our experience shows that wireless LAN is very sensitive to radio-conditions, orientation of the antenna, presence of people etc. For TCP, throughput variations were even greater. Results in Figure 2 show that as the length of the route increases, the possible throughput decreases as expected. However, in routes containing more than two nodes, the throughput can decrease almost to 0 kbits/s. This can be explained by the known problems of TCP in a wireless environment. Higher BER on the path can trigger TCP’s congestion control mechanisms. In ad-hoc networking these problems are enhanced by the fact that routes must be established/re-established, which can introduce extra delays that TCP can misinterpret as lost packets due to timeout mechanisms also triggering the congestion control mechanisms [8]. Reducing TCP window size to one packet only or certain TCP modifications should give better performance.

VI Conclusion

Substantial variation in results was observed during tests. This can be attributed to the radio environment – our experience shows that wireless LAN is very sensitive to radio-conditions, orientation of the antenna, presence of people etc. For TCP, throughput variations were even greater. Results in Figure 2 show that as the length of the route increases, the possible throughput decreases as expected. However, in routes containing more than two nodes, the throughput can decrease almost to 0 kbits/s. This can be explained by the known problems of TCP in a wireless environment. Higher BER on the path can trigger TCP’s congestion control mechanisms. In ad-hoc networking these problems are enhanced by the fact that routes must be established/re-established, which can introduce extra delays that TCP can misinterpret as lost packets due to timeout mechanisms also triggering the congestion control mechanisms [8]. Reducing TCP window size to one packet only or certain TCP modifications should give better performance.

Figure 1. The maximum chain throughput

Figure 2. TCP throughput
the testing of a live ad-hoc network are presented as well.

“Rutiranje u ad-hoc mrezama”,
Marina Dupcinov, Srdjan Krco