Mesh Cluster Based Routing Protocol: Enhancing Multi-hop Internet Access using Cluster paradigm

Radosław Olgierd Schoeneich and Marcin Golański
Institute of Telecommunications, Warsaw University of Technology, Warsaw, Poland,
e-mail: {rschoeneich, mgolanski}@tele.pw.edu.pl

***Abstract*—The purpose of this document is to describe an approach to using the clustering paradigm in a routing protocol for multi-hop ad-hoc wireless networks with Internet Access. In the Mesh Cluster Based Routing Protocol (MCBRP) wireless nodes are grouped into clusters with a cluster-head responsible for communication management. Moreover an existence of special cluster-heads called hard-cluster-heads has been assumed. Hard-cluster-heads have the functionality of an interface between wireless and other types of network, usually the Internet. This paper describes each node type: cluster-member, cluster-soft-head, and cluster-hard-head. Furthermore assumptions, used solutions and discussion have been presented.**

***Keywords*—Wireless LAN, MANET, mesh networks.**

I. Introduction

Nowadays, Wireless Local Area Networks (WLAN) are very popular and useful in many aspects of portable devices communication. Access to the network (i.e. Internet) is mostly provided in a single hop, which limits the radius of a typical IEEE 802.11 access point (AP).

The range limitation has an influence on the number of APs. Many access points are required to cover large areas. The problem occurs when users need an Internet connection in areas without a fixed infrastructure, such as: (a) trains and car tunnels, (b) large outdoor areas like golf-polls or garden-plots near hotels, (c) all emergency situations. The examples have a common feature: provide connectivity for every person, who need it? One of the possible solutions is multi-hop access to the Internet without range limits. To extend the provided range the every node must act as a router. This topology is called a "mesh". Today, there is a number of routing protocols for multi-hop wireless networks. Very few of them assume an existence of gateway nodes. To the best of our knowledge, a cluster-based structure is not used in existing solutions. In this paper we present a proposal of a multi-hop routing protocol based on the Cluster Based Routing Protocol – CBRP[2]. For this reasons we call our proposal Mesh-CBRP.

The rest of this paper is organized as follows. In Section 2 we shortly present and discuss the CBRP ad-hoc routing protocol and the approach to modifying. Full description of assumptions and functional changes is presented in section 3. Section 4 contains information about implementation and measurements. In Section 5, we shortly present related work. Section 6 includes a summary and conclusions.

II. Modyfications of the Cluster Based Routing Protocol

The Cluster Based Routing Protocol (CBRP) [2] proposed by Mingliang Jiang et al. is a protocol which uses the clustering paradigm. It integrates proactive and reactive features. The main approach is to divide all nodes in the network into overlapped or disjointed clusters. Each cluster has its own cluster-head (CH) which maintains information about nodes in its direct neighborhood. Remaining nodes are called cluster-members (CM). The Cluster-head is elected by a cluster election algorithm. Changes of node status are made if a CH disappears, or two CH are hearing each other. Routing between clusters is done using a reactive scheme, using membership information maintained by CHs. The Clustering paradigm helps in minimizing the flooding during route discovery phase. The CBRP also solves that issues as route maintenance, broken link handling and unidirectional links.

A. CBRP modifications

After a detailed analysis of CBRP advantages and disadvantages, changes of several attributes have been suggested.

(a) We do not support unidirectional link maintenance. In WLAN this mechanism is not necessary because of using acknowledge messages (ACK). A node which receives a packet has to send an ACK to the sender. Therefore we assume bi-directional links.

(b) We propose to use three state node roles (Undecided, Member and Head), new role called cluster-hard-head (CHH). It is assigned to gateways to the Internet. This implies that we have to change the hierarchy, relations between nodes, and the cluster election algorithm.

(c) We propose to use a simple mechanism for dynamic address assignment with duplicate address avoidance.

To keep our assumptions, changes in the structure of CBRP frames were necessary. For example, we don't need a link field, we merge link and role field into new role field with 2 bytes length. Moreover several changes to request, response and error frames were proposed.

III. Mesh-Cluster Based Routing Protocol

A. Assumptions

This section describes the main assumptions of the M-CBRP. In our proposal two basic functions should be provided: (a) every CM should have access to the Internet, even if it takes many hops - it means that every node has

to participate in the routing process; (b) a mechanism of automatic data forwarding from a CHH with broken link to the Internet to another CHH is required.

Other assumptions, which help us make our proposal easier and more complete, are: (a) all nodes should work in ad-hoc mode; (b) as many CHH's as possible should be used; (c) communication principles between CM's and CHH are required; (d) a simple mechanism of checking ability to be a gateway should be implemented at every CHH; (e) we use DAD (Duplicate Address Detection) algorithm for address assignment [10] [11].

B. General Description

The proposed protocol, groups mobile nodes into clusters. Each cluster has a node, which manages information about it. This special node can be elected from all nodes in the cluster. Therefore it is called cluster-soft-head (CSH). Some nodes, like AP's or gateways, can manage clusters but do not participate in the election process. We call them cluster-hard-heads (CHH). The role of CHH is fixed and can not be changed. It is important that CHH can communicate with other CHHs, therefore overlapping clusters are allowed – Figure 1. As was described in previous sections, remaining nodes are cluster-members (CM). Nodes without cluster assignment are denoted as undecided-nodes (UN).

Similar to CBRP, proactive knowledge acquisition about network topology by CMs in each cluster is required. Each CM simply sends HELLO messages as a broadcast. This message has a format taken from CBRP, but we do not use link status field. Moreover a role field has been expanded.

At first, in order to find the destination node, a route cache at the originating node should be checked. If there is no current path information, a Route Request message (RREQ) is sent.

When a CHH receives a RREQ, the destination address from the packet header is checked. If address belongs to the global pool of addresses, it means that the destination node is located outside of the MANET network CHH then sends a Route Response (RREP) message as an answer for RREQ. If the address is placed in the local pool of addresses, it means that it can still happen, that the destination node is outside of network, but CHH has to check it using ICMP. The CHH encapsulates RREQ within ICMP_REQUEST frame and then sends it to the fixed network.

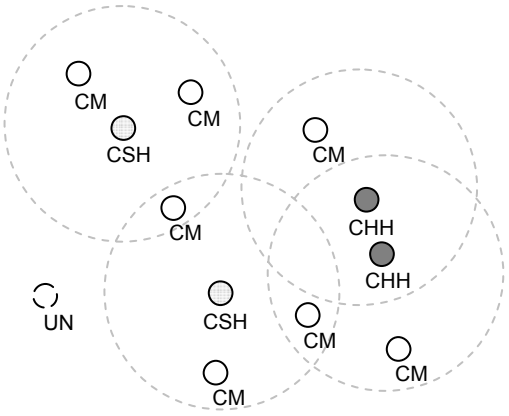

Fig. 1. Different node types in M-CBRP protocol.

Each destination node sends a RREP answer. The format of RREQ and RREP headers is similar to what has been proposed in CBRP. However, a different algorithm of the frame content assignment has been used. After receiving a RREP message, the originating node can start data transmission. Source route header and list of intermediate nodes IP's is copied to the data header and sent through the network.

All the time, CHH must check ability to be a gateway for another network. Therefore, CHH use ICMP protocol also.

In our proposal, we use CBRP broken link handling with link reassignment and error-information packet (ERR) sending.

C. Address Assigment

After node initialization, according to the proposal, IP addresses are assigned at random scheme. User can set up fixed address if it is necessary. A new node listens the all HELLO messages during the first HELLO_BROADCAST intervals. If another node has the same IP address, the random address assignment procedure should be repeated. Consequently, if a new node does not hear any HELLO message with the same address, it floods a network with a RREQ message with the address_assign field set to *true*. If any node has the same address, the new node receives RREP message as an answer. This process is repeated after each ADDRESS_INTERVAL time. It is necessary, for example when two subnetworks become interconnected.

D. Gateway functionality assignment

We propose to use the ICMP protocol for checking the ability of a node to be a gateway to the Internet. CHH can periodically send an `ICMP_ECHO` message to well known Internet servers (chosen by configuration). We suggest using at least two servers for redundancy. In this case, CHH can not be a fully functional gateway if does not receive four messages (two per server). This situation causes, that the node has a CHH status, but works as a CSH (all packets are forwarded into wireless link only). All the time, CHH periodically sends `ICMP_ECHO` packets and it waits for an answer.

E. Route discovery, response and data forwarding

A new algorithm of route discovery has been proposed, which uses a table of neighborhood nodes (in two hops range) and a route cache. Every node maintains information about the newest and the shortest paths to other nodes. For this mechanism, nodes use *data frame* header, which always contains current path. We consider this solution safe, because this way we take into account only active and used paths. As nodes can move frequently, the route cache is refreshed every 30 seconds.

In case when proper information is not available in the route cache, the *source node* can use a route request message RREQ to find the path to the *destination node* – Figure 2. As an answer to the RREQ message, the *destination node* generates a route response message RREP. With this procedure we introduce the general idea of pairs of request/response messages in cluster paradigm networks.

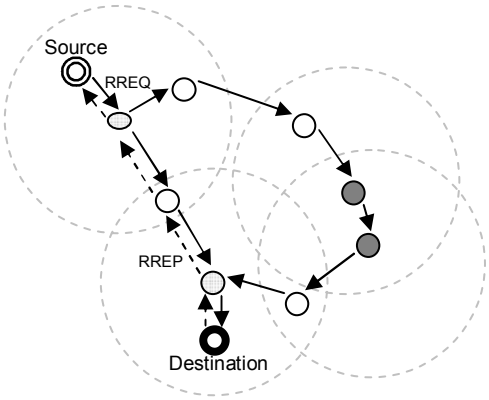

Fig. 2. Example of using RREQ/RREP messages pair.

As stated earlier, a new `address_assign` field has been proposed. It is used to recognize: (a) request for address (`address_assign = true`); (b) request for route discovery (`address_assign = false`).

To reduce RREQ packets traffic, each next (repeated) RREQ packet is sent after a double time from the previous, i.e. the second RREQ packet is sent after 0,5 sec., third after 1 sec., fourth after 3sec. etc. This process recurs every 20 seconds. With our best knowledge, this solution is not expensive.

We assume propagation of RREQ packets between two CHHs. Thus, if a CHH is placed in the neighborhood of another CHH a special algorithm should be used. In such case the CHH acts as a gateway to cluster head (member node) and as a cluster head simultaneously. Therefore it writes its address twice in the packet header. One position determines where the packet should be forwarded, the second determines through which member node.

The CHH can communicate via fixed networks. Therefore it uses ICMP [8] messages. We propose encapsulation of RREQ messages into `ICMP_ECHO` packets in order to send them via wired network to other CHHs. For this purpose, a special IP address (i.e. `0.0.0.0`) to distinguish transition between the wireless and the fixed network segment is used. It acts as an address of the gateway between two CHHs.

As mentioned above, when the destination address belongs to a public pool, CHH should answer with a RREP message. Otherwise the RREQ message is capsulated into `ICMP_ECHO`. Based on the received `ICMP_ECHO_RESPONSE`, the CHH knows if the destination node is located in a fixed network segment (`ICMP_ECHO_RESPONSE` packet includes encapsulated RREQ message sent for CHH). Figure 3 shows the main idea of this solution.

Communication is initialized by the node placed on the fixed network segment, it begins with an `ARP` [7] message first. CHH forwards this packet through the wireless interface and waits for a RREP. Afterwards, it sends an `ARP` answer to the origin.

We presume that a node which receives a RREQ should answer only once. The RREP propagates on a reverse path. Every cluster head (CSH, CHH) in the middle of the network, can try to shorten the path i.e. in the case of a wrong address assignment. In consequence, an origin node receives a RREP with the shortest path in terms of number of hops.

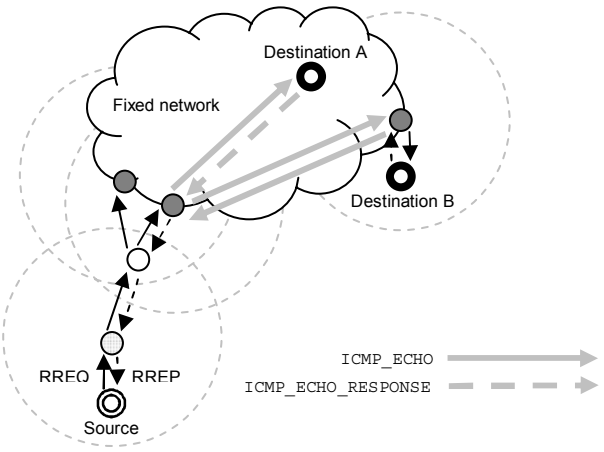

Fig. 3. Encapsulation of RREQ messages.

A DATA frame consists of a header including all IP addresses in the path (taken from the RREP or *route cache*), and the tail. This type of frame propagates hop by hop according to the header information. Every node with knowledge required to make the path shorter can modify the header content.

IV. Implementation and Measurements

For the implementation, the C++ language and the GNU/Linux OS as an execution environment have been used. BSD sockets API was used for communication with the wireless card and TAP driver to communicate with the computer. A Standard frame in LAN has length of 1500 bytes, while the maximum M-CBRP header has 256 bytes. Therefore the data field can not be longer than 1244 bytes.

The general view of the M-CBRP implementation architecture has been shown in Figure 4.

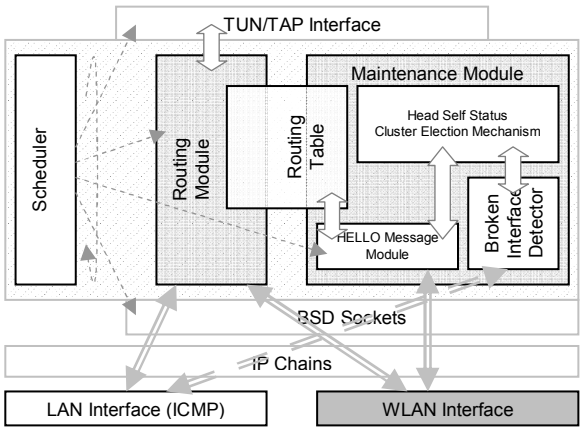

Fig. 4. M-CBRP implementation architecture

Main engine of implementation acts as a linear scheme scheduler, which serve all socket interfaces in sequence. The scheduler has to handle two main software components, which are responsible for routing packets and maintenance. The main goal of the *Routing Module* component is to handle all packets coming from the TUN/TAP [4] interface and the BSD Socket. The main object of this component is the *Routing Table* which is require for the *Maintenance Module*. The *Maintenance Module* is responsible for sending `HELLO` messages and

managing the current role of the node, which is determined using information from the *Broken Link Detector* and the *Hello Message Module*. The *Hello Message Module* communicates with the NOS using raw type of *BSD Socket* to the *WLAN Interface*. The *Broken Link Detector* also uses *BSD Socket*, but using ICMP to communicate with the wired network. The *Routing Module* uses two kinds of *BSD Sockets*: raw for WLAN communication and ICMP [8] for the wired interface. To avoid unnecessary `ICMP_replay` messages between CHHs, *iptables* was used. The *iptables* are also useful for NAT translation.

For the measurements, a small network with 3 nodes A, B and C, arranged in a straight line, has been built. We measure traffic received at Station A from Station B and C respectively. The middle Station (B) was responsible for forwarding packets between stations A and C. To generate the traffic, the well known *IPerf* tool has been used on each station. Because of early state of the implementation the aim of the experiment was not to check solution efficiency, rather to check if it works properly. The results have been illustrated in Figure 5 and 6.

Because of buffering implemented at each station, the generated traffic is not flat in term of throughput and varies dynamically. Generally Station B has about twice more bandwidth available. The radio channel of Station C was occupied for 3 seconds (from 5 to 7 on Figure 5). In the same time Station B tried to send all aggregated packets including packets received earlier from Station C – Figure 6.

The tests show that implementation works properly. Delays of data transmission were not significant. Moreover, results show that M-CBRP protocol is functional and can be verified in larger networks.

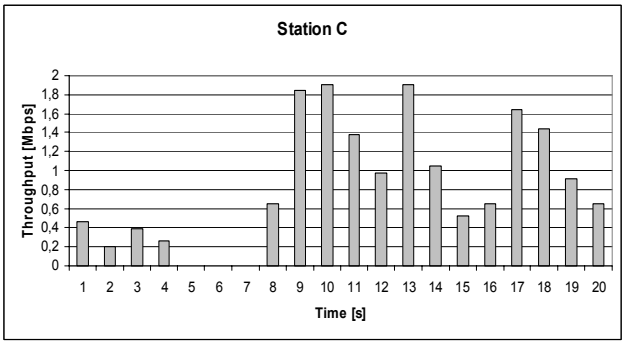

Fig. 5. Traffic received from Station C.

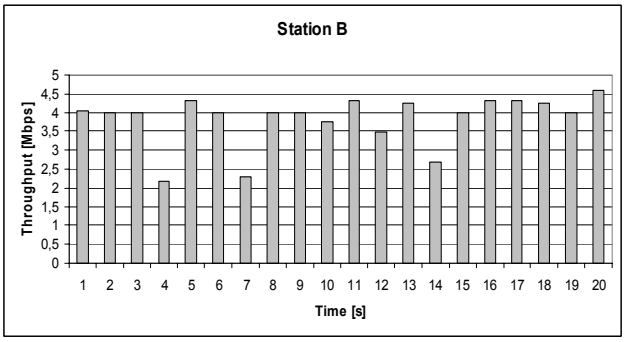

Fig. 6. Traffic received from Station B.

V. Related Work

The MCBRP routing protocol proposal is based on CBRP. In the article, we have analyzed other routing protocols like DSR [3], AODV [6], LUNAR [9], CGSR [1]. We do not use sophisticated optimizations because of basic assumptions concerning simplicity. Thus a simple mechanism with randomized address assignment has been proposed.

Furthermore, we evaluate a few mesh-based proposals. In [4] authors propose complete mesh-worked network project. They use characteristics of the AODV protocol and suggest K-hop radius paradigm. AP takes a path proactively to all their nodes, but every node finds the path reactively. The DHCP protocol is used. Their proposal was implemented under GNU/Linux and works in ad-hoc mode.

Another proposal is the Wireless Mesh Routing (WMR) [10]. Authors base on the Ad-hoc QoS Routing protocol (AQOR). They tried to serve QoS in mesh based networks. The proposal was simulated in OPNET modeller.

VI. Conclusion

A simple solution to merge an extended routing protocol based on CBRP and the APs or gateways to the Internet has been proposed. Differences of nodes behaviour between proposal and original CBRP protocol have been described. In our proposition we suggest various optimisations and we describe protocol details.

References

[1] Chaing C.C. , H. K. Wu, M. Gerla "Clusterhead gateway switch routing protocol" (CGSR), gerla-routing-clustered-sicon97.pdf

[2] Mingliang Jiang, Jinyang Li, Y.C. Tay, "Cluster Based Routing Protocol (CBRP)", draft-ietfmanet-cbrp-spec-01.txt, August 1999 http://www.comp.nus.edu.sg/~tayyc/cbrp/

[3] Johnson D., Maltz D. "Dynamic source routing protocol, draft-ietf-dsr-06.txt", http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-06.txt

[4] Krasnyansky M. "Universal TUN/TAP device driver" http://vtun.sourceforge.net/tun/

[5] Miller M.J., W.D. List, N.H Vaida "A Hybrid Network Implementation to Extend Infrastructure Reach", University of Illinois, Tech rapport 2003. http://srhc.uiuc.edu/ńhv/papiers/hibrid-tech.pdf

[6] Perkins C. "Ad hoc on demand distance vector routing protocol, draft-ietf-manet-aodv-09.txt", http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-09.txt

[7] Plummer D. RFC 826 "An Ethernet Address Resolution Protocol" 1982, http://www.ietf.org/rfc826.txt

[8] Postel J. RFC 792 "Internet Control Message Protocol" 1981, http://www.ietf.org/rfc792.txt

[9] Schudin T. "Lightweight Underlay Network Routing Protocol", http://www.docs.uu.se/selnet/lunar/manet-lunar-00.txt

[10] Qi Xue, Laura Ganz, Wireless Mesh Routing, "QoS routing in Mesh-based Wireless LANs" International journal on Parallel and Distributed Computing, vol 9 p179-190 2002

[11] Sanket Nesargi, Ravi Prakash, "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network", Proc. INFOCOM 2002, June 2002

[12] Charles E. Perkins, Jari T. Malinen, Ryuji Wakikawa, Elizabeth M. Belding-Royer, Yuan Sun "IP Address Autoconfiguration for Ad Hoc Networks", Internet-Draft, draft-ietf-manet-autoconf-01.txt, November 2001