Peer-to-peer network technology applied to the harbour environment

G.Dodero, V.Gianuzzi, D.Venzano
DISI, Universitá di Genova
Via Dodecaneso 35
16146 Genova, Italy
(dodero,gianuzzi)@disi.unige.it

F.Giacalone, F.Parodi
Fantuzzi Reggiane S.p.A.
Via Renata Bianchi, 40
16152 Genova, Italy
francesco.giacalone@fredreggiane.com

Abstract

This paper describes an experience in the development of a network, based on peer-to-peer and wireless technologies, explains the choices, and compares this approach to the traditional, infrastructure based, wireless network.

The environment hosting such a wireless network is a challenging one, that is an harbour area in Southern Italy. Hardware, software and especially dynamic routing protocols have been evaluated for suitability to such an environment. The choice of a cheap, consumer level hardware equipped with a customized Linux and OLSR protocol have proven sufficiently robust for actual deployment. The experience results from a cooperation of a university department, DISI, and a company, Fantuzzi Reggiane.

Keywords: wireless networks, mobile ad hoc networks, multi-hop peer-to-peer networks, dynamic routing protocol, embedded Linux, harbour areas.

1. Introduction

Wireless networks already have many advantages over wired technologies in the harbour environment and are deployed all over the world. So far, as to the authors' knowledge, all such deployments rely on an infrastructure-based approach, that is, by installing access points, or base stations, at specific fixed locations. On the other hand, this paper describes how peer-to-peer technologies may be used to create a communication system able to transport TCP/IP traffic in a very peculiar environment, a harbour container terminal. This environment has a set of special characteristics:

- large, flat areas, usually divided into load/unload and stocking zones. Each zone is optimized in space to contain as many containers as possible;
- harbour container terminal are characterized by strong electromagnetic background arising, due to the use of radar, VHF/UHF radio devices, and to the huge amount of metallic object in the ares
- moving machinery of all kinds, from small passenger-only cars to big ship-to-shore cranes
- extreme weather conditions, temperature, humidity and salinity
- uninterrupted activity 365 days a year, 24 hours a day
- terminal activity delays must be kept at minimum to prevent disruption of ships or trains timetables, and money losses
- the position of every container stocked in the terminal must be constantly tracked, for accountability and insurance reasons

The TCP/IP network should be able to provide continuos communication between the moving machinery and the central office to exchange moving orders, container and GPS data, diagnostics and maintenance data.

The moving network nodes and the realtime requirements fit perfectly for the use of a wireless network, which has the ability to provide constant network availability. Among the different wireless standards existing today, WiFi [1] was chosen for cost reasons and easiness of purchase, but also to provide backward compatibility in existing installations. In particular the 802.11b incarnation of WiFi was chosen, instead of the more modern 802.11g, because of the greater communication range and of the difficulties encountered trying to find a stable driver under Linux for 'g' devices. The 11Mbit/s bandwidth is, in any case, more than enough to support the average load the network will have to bear.

Other wireless technologies were evaluated, such as ZigBee (802.15.4) [2] and WiMAX (802.16), but were discarded for availability reasons, and also for costs (10 times more than WiFi). In particular WiMAX would offer greater communication range and interference resistance, while ZigBee would provide ad-hoc networking capabilities integrated in the data link layer.

Traditionally WiFi is deployed in infrastructure mode, installing access points in fixed locations (i.e. on top of light poles), connected to an underground ring of optic fiber. All other nodes are configured as clients and can roam among the access points using proprietary and non standard protocols. This type of deployment has several drawbacks: if an access point fails all the nodes present in the area that was covered by its signal stop communicating and must move somewhere else to regain that ability.

Some fault tolerance can be achieved by installing the access points so that the areas they cover overlap, but access point redundancy is limited, for cost reasons and because clients can get confused by too many strong signals. Also, the installation and extension of such an infrastructure is difficult because it needs the installation of underground cables, a very costly operation since it requires the digging of very deep trenches to prevent damage from the great weight of the machinery circulating in an harbour terminal.

To get over these problems we decided to use the WiFi protocol in Ad-Hoc mode [3] and a dynamic routing protocol able to update the IP routing tables and provide the multi-hop capability that simple Ad-Hoc is lacking. This kind of network structure has all the advantages of wireless networking, plus a built-in fault resistance. Indeed nodes can use each other as a bridge to reach destinations non in line of sight(NLOS), and minimum cabling is needed. All nodes, i.e. mobile nodes (moving machines), repeater nodes (fixed repeater) and the nodes directly connected to the wired network (called mesh wired nodes in the following) are equivalent, with no distinction in hardware nor software configuration, thereby lowering the maintenance cost of such a network. All nodes are a part of the wireless network, whose capacity and coverage area shall dynamically adapt in accordance with the machine usage scheme. A peer-to-peer network is characterized by alternating areas of respectively high and low density of nodes. In high density regions the bandwidth request is high, but the number of service routes is also high, so that access to a mesh wired node is always possible. In the harbour environment, high density zones are usually the load/unload areas, while the stocking places show a lower density of machines.

When a mobile node moves, the traffic changes and the service routes in both the outgoing and the incoming regions re-adjust, in order to balance the new amount of traffic. This is known as dynamic load balancing, and it is typical of wireless ad-hoc networks, as opposed to what happens to wireless networks in infrastructure mode. So, the performance of the ad-hoc network increases as the number of nodes increases. A broad-band telecommunication system is built up in such a way, by a number of heterogeneous entities which interconnect to each other and provide common advantages. Note also that in expanding harbours the machine fleet is in constant increase, and the network in turn is capable of scaling up.

We decided to call MeshAP the node of this ad-hoc network, as a product name. This has nothing to do with the Access Point mode of the 802.11 protocol, as above explained.

2. Hardware

Since our primary objective is to build a completely functional network node, to be replicated many times, the first step was deciding the hardware platform the node will be based on, and its requirements for standalone operations.

The MeshAP would be installed, the first time, near Nola (NA) at the Interporto Campano. Climate conditions there are not very extreme, but it should be kept in mind that for its own very nature the MeshAP has to be installed in an exposed position. So we expected a temperature range from -5C to 70C (a closed, metal box, in the direct light of the sun in south Italy). Some nodes would be installed on moving machinery, where the diesel engine would provide all the required electrical power, but that same engine would provide a great amount of vibrations during all the activity.

One possibility was to make use of components already in use in Fantuzzi Reggiane, i.e. a small PC, called BlueBox, with no moving parts, a PC 104 system bus and a PCMCIA port for addon cards, such as a wireless card. The BlueBox was already studied and tested to withstand the harshness of the environment in which it would operate, but its high costs pushed for a more economical solution. So we tested the possibility of using very low cost hardware, consumer grade (about 10 times cheaper than a BlueBox). In particular a Linksys wireless router, the WRT54G, was used since it is possible to change the firmware with a Linux distribution. We tested its functioning in a thermal room, and the results showed that it was working quite well, so the BlueBox solution was discarded.

2.1. Components

The wireless router is installed inside a sturdy box with a small electrical resistance and a thermostat that provides the heat necessary to prevent sub zero temperatures. As a matter of fact, tests conducted in the thermal room pointed out that the WRT54G was very sensible to low temperatures with a noticeable slow down in the wireless activity under 5C and a complete hang under 0C. Instead high temperatures would not pose any problem: at 65C all the router components would work as usual.

The WRT54G is based on a MIPS CPU, a Broadcom wireless chip, 4MB of flash for the operating system and 16MB of RAM. As I/O a five port ethernet switch is provided, and two serial ports are available soldering to the base board a small additional chip.

The big endian architecture and the small long term storage space require a special operating system, recompiled to work on the MIPS architecture and optimized for size.

3. Software

A GNU/Linux distribution called OpenWRT was chosen as base for the MeshAP operating system. There are few OSes available for the MIPS architecture and most of them lack driver support for the devices in the WRT54G. Others require licensing costs that we were not willing to pay. So Linux was taken almost automatically, moreover its Open Source philosophy permits a great flexibility in adapting existing software to the particular needs of the MeshAP application.

3.1. OpenWRT

OpenWRT is a distribution prepared for a number of devices from Linksys, Netgear and Asus with similar characteristics. It features a packaging system and a build environment to compile new programs, providing the base framework for building a complete software environment.

The packaging system is `ipkg`, already in use by many PDA distributions; it provides a way to install new software on a running system, without having to prepare a new firmware image to be written on the flash.

The build system provides a complete toolset for doing cross compilation from a system running on any architecture to MIPS, to port new software written in C or C++ to the OpenWRT environment.

Other, similar, distributions exist for the same hardware. They are built with different packaging systems and are thought for very specific applications. Some of them require also the payment of a small fee to be able to download updates and the latest versions.

3.2. Dynamic routing

A thorough research has been made to find and catalog all existing implementations of dynamic routing algorithms. The result is that only AODV (Ad-hoc On-demand Distance Vector) and OLSR (Optimized Link State Routing) have an implementation that is enough advanced to be used in a production environment. Also AODV and OLSR are being standardised and are currently available in RFC form.

AODV [4] is a reactive protocol that is able to build a new routing path every time a new connection is made. Some caching mechanisms permit to reach a good interactivity speed in spite of the built-in delay each time a communication is initiated. To be able to catch connection attempts AODV needs to run some code in kernel space [5] . This was considered by us a major drawback because Linux kernel APIs are not stable, even between minor release versions, and the work needed to keep AODV up to date would be too much.

OLSR [6] is a daemon running completely in user space, being a proactive protocol it builds the routing tables during the initialization time and then maintains them by exchanging continuously messages with its neighbours. This causes a certain (small) amount of bandwidth to be occupied by OLSR messages, even when there are no communications, but a network path to reach every known destination is available in each instant, causing no delay when establishing new connections.

OLSR was chosen also because its older version [7] was already available for OpenWRT, and this shortened the time required for porting the latest version to our system.

3.3. Diagnostic software

Two applications were written to permit remote management and diagnostics of each node, they are based on a client/server architecture: each node runs a server process, that acquires data during the node normal activity. The client is run by the system administrator, and it shows the realtime status of all nodes available in the network, by connecting to each server process and requesting the data at fixed time intervals. This client application may also build a graph of the wireless network, showing which nodes are connected and their IP addresses. Thanks to the flexibility of OpenWRT, each node also runs a small HTTP server, that provides a web interface used for configuration and monitoring tasks.

3.4. Network infrastructure

Each MeshAP is configured to use a combination of proxy ARP and HNA OLSR messages to achieve a complete transparency: two hosts connected by a MeshAP network don't require any special knowledge to communicate with each other, only the basic configuration of IP addresses is needed. The MeshAP network behaves as a switched cabled network, modulo latency issues.

HNA messages provide a way for an OLSR node to advertise its capability to reach another subnetwork, in the IP sense. Each node that receives an HNA message adds an entry to its routing table stating that to reach the advertised subnetwork, packets should be sent to the HNA sending host. They take care of one way of the communication, from the MeshAP network to a non-OLSR node.

The path from a non-OLSR node to the MeshAP network is provided by proxy ARP, a technique where each node forwards an ARP request received on one interface to another if there is a matching entry in the IP routing table. This feature is provided by the Linux kernel, and it allows IP address resolution between hosts that are not on the same ethernet collision domain.

4. Application at the Interporto Campano, Nola (NA)

The Interporto Campano is a new structure being built just outside the town of Nola, near Naples in south Italy. It provides structures for the loading/unloading of goods from containers, customs areas, and a large (1,5Km x 500m) area where containers are stocked and loaded on trains and trucks. This place is where the wireless network was requested. There, at least two stackers (container moving machinery) move, receiving and transmitting data about containers codes, positions and weights. Also some maintenance informations can be requested through the network about engine status, oil pressure, temperatures and so on.

The project that is to be implemented in january 2006 positions three MeshAP nodes on fixed locations, on top os light poles, at an height of about 20 meters, spaced between 300 and 400 meters from each other. These nodes provide a wide distribution of the wireless signal all over the terminal. On each stacker an additional MeshAP is connected, so that they can communicate directly with the fixed nodes, or act as bridges for each other if there are visibility or interference problems. Figure 1 shows the final positioning of the MeshAP and its antenna on a stacker.

The container data processing and display application was not part of this study. It is a remote desktop application that will be relayed through the MeshAP network to the stacker operators' displays via the VNC protocol. The operator will be able to interact with the system by using a touchscreen.

5. Final tests and conclusions

The MeshAP system is undertaking some real-world testing [8] before being deployed at Nola, currently foreseen for January 2006. So far it passed all the initial prerequisites regarding cost effectiveness, easyness of installation and operative range. The completed MeshAP, with its metal box, was able to function flawlessly for some hours at an external temperature of -15C.

Field tests were performed on a 4 nodes network, with two fixed nodes installed on the roofs of a building, and creating paths of varying length by moving two nodes on cars. The test environment was especially noisy, with moving trucks and containers, which caused some reflections. The routing protocol proved itself sufficiently robust to maintain connectivity in such an environment, once a few tuning parameters have been set. Specifically, the *Hysteresis* parameters needed to be tuned differently, with respect to lab testing, because of the relative stability of network topology (vehicles move slowly). Two threshold values, as set in the lab, were found to be too close, causing a quick reaction to ”topology changes”, which in fact were spurious reflected signals, caused by moving containers.

During such field testing, some small latency issues were noticed, caused by packet retransmission by each node on the same radio channel. This problem can be easily solved by developing networks with a small maximum radius, in terms of hops. Empirically, a number of 4 or 5 hops was determined to be the maximum, and for the Nola area that would be enough. In larger future installations, it shall be sufficient to use protocols that provide more bandwidth (i.e. 802.11g or WiMAX) in order to bring that figure up.

Concluding the MeshAP system has many advantages over the traditional, infrastructure operative mode. The system is able to provide transparent communication between mobile and fixed nodes, without the need for installation of underground cabling. It has fault tolerant characteristics, since nodes can dynamically reroute connections when a malfunctioning node is detected without human intervention.

Also, the low costs of each node, its simple installation, and self-diagnostic features make the MeshAP a very competitive solution.

References

[1] W. Alliance, (2003), Wi-fi protected access: Strong, standardsbased, interoperable security for todays wi-fi networks [Online]. Available: http://www.wifi alliance.com/OpenSection/pdf/ Whitepaper_Wi-Fi_Security4-29-03.pdf

[2] W. C. Craig, (2004), Zigbee: wireless control that simply works [Online]. Available: http://www.zigbee.org

[3] D. A. M. David B. Johnson and J. Broch, *Ad Hoc Networking*, Addison-Wesley, 2001.

[4] B. W. Erik Nordstrom and H. Lundgren, (2002), AODV-UU [Online]. Available: http://core.it.uu.se/AdHoc/AodvUUImpl

[5] W. C. T. G. NIST, (2001), Kernel aodv [Online]. Available: http://w3.antd.nist.gov/wctg/aodv_kernel/

[6] T. Clausen and P. Jacquet, (2003), RFC 3626 - Optimized Link State Routing Protocol (OLSR). Technical report, Network Working Group, Project Hypercom INRIA [Online]. Available: http://www.rfc.net/rfc3626.html

[7] A. Tonnesen, *Implementing and extending the Optimized Link State Routing protocol. Masters thesis,* UniK - University Graduate Center, 2004.

[8] D. Venzano, *Dynamic routing algorithms applied to wireless networks in harbour areas. Masters thesis*, University of Genova, 2005.