A Network Architecture for Mobile Robotics

Paulo R.S.L. Coelho[1], **Daniel H. Moraes**[1], **Eliane G. Guimarães**[2]
Eleri Cardozo[1], **Thienne Johnson**[1], **Fernanda C.A Atizani**[1]

[1]School of Electrical and Computer Engineering
University of Campinas
13083-970 – Campinas – SP

[2]Division of Robotics and Computer Vision
Information Technology Center Renato Archer
13083-970 – Campinas – SP

pcoelho@dca.fee.unicamp.br

Abstract. *Mobile robotics environments must adopt networking solutions that provide secure and reliable communications for mobile robots across wide areas such as hospitals, factories, farms, etc. This paper proposes a network architecture for large mobile robotic environments built above the existing networking infrastructures. The architecture relies on an overlay network built above an already deployed network. The overlay network must fulfill the requirements demanded by mobile robotic applications, mainly, communication continuity during handover, security, and quality of service. A prototype of this architecture was implemented and evaluated in a mobile robotic environment composed of Pioneer P3-DX mobile robots accessed through the Internet or high speed private networks such as the RNP/Giga and Fapesp/KyaTera networks. Results from simulation show that the architecture scales well in larger networking scenarios.*

1. Introduction

As mobile robots become more and more integrated on internal and external environments, networking solutions for supporting control and communication with the mobile robots are of major concern. Buildings, factories, and hospitals, for instance, already have networking infrastructures deployed. Usually, these networks follow the common architecture where a backbone integrates a set of departmental subnetworks. Departmental subnetworks usually incorporate wireless access points for mobile clients.

Handover is the process by which a mobile node changes its network point of attachment in order to improve the signal-to-noise ratio of the wireless link. A layer 2 (L2) handover rebuilds the wireless link established with the previous access point to an nearby access point. During this process the mobile node remains unreachable. The handover overhead (time to resume communication) varies from tens of milliseconds to seconds [Vatn 2003] depending on the wireless hardware and device drivers installed on the mobile nodes and access points. After the L2 handover has been completed, the layer 3 (L3) handover starts. L3 handover rebuilds the L3 parameters such as IP address, network prefix and default router. If the L3 parameters of the mobile node change (i.e., the new access point belongs to a different subnetwork) the transport connections established on

the previous subnetwork are broken. For mobile robots, that commonly act as servers, changing L3 parameters is obviously unacceptable.

If the organization decides to deploy mobile robotics applications without constraining the mobile robots inside a subnetwork, a new network architecture must be designed and deployed. This architecture must offer communication continuity during handover, security, and quality of service to the mobile robots. An expensive solution would deploy a separated network for the mobile robots. A more economical approach is to build a logical (overlay) network above the existing organizational network able to fulfill the mobile robotics requirements. Fig. 1 illustrates this approach. The overlay network may need some low cost devices such as access points and PC-based servers that are connected to the existing network as any other devices. As such, the architecture makes use of the existing expensive devices such as routers, switches, and cabling without demanding any updating or reconfiguration on these devices.

The overlay network gives the mobile robots an homogeneous networking environment where parameters such as ESSID (Extended Service Set ID), network prefix, default router, and security keys remain unchanged. As a result, mobile robots can roam among access points preserving their network connections.

This paper is organized as follows. Section 2. presents the proposed network architecture for network robotics. Section 3. presents some implementation details of this architecture. Section 4. describes an application on network robotics running above the architecture. Finally, Section 5. presents the concluding remarks and a comparison with a related work.

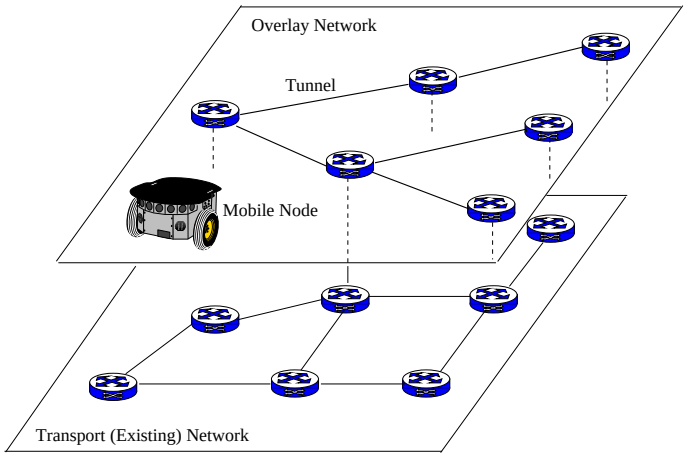


Fig. 1. An homogeneous overlay network built above an heterogeneous transport network.

2. A Network Architecture for Mobility

A network architecture addressing mobility must provide a set of mobility-related functions. The most important functions are:

- L3 addressing functions: functions that assign L3 parameters to the mobile nodes while they roam among access points.
- Location functions: functions that keep track of the mobile nodes and signal the network when they change their points of attachment.

- Mobile routing functions: functions that act on the network in order to deliver packets to the mobile nodes' actual location.
- Forwarding functions: functions that allow special packet forwarding decisions such as packet filtering, address translation, tunneling, and proxying.
- Management functions: functions that allow routers be configured to perform the mobility-related functions (e.g., the establishment of tunnels).
- Enhancing functions: additional functions that provide fast handover, quality of service, security, reliability, etc.

The Mobility Plane Architecture (MPA) [Zagari et al. 2008, Zagari et al. 2009] is a network architecture for supporting mobility in IPv4, IPv6 and MPLS (Multiprotocol Label Switching) transport networks. In MPA, mobile routing functions are performed by the Resource Reservation Protocol (RSVP) with two extensions:

1. Traffic Engineering extensions that allow constraint-based routing of tunnels (RSVP-TE) [Awduche et al. 2001].
2. Point-to-multipoint (P2MP) extensions that allow the signaling of P2MP tunnels [Yasukawa 2006].

RSVP-TE nodes define a logical (overlay) network above the transport network. The overlay network is composed of a set of P2MP tunnels rooted on the ingress routers. These tree-structured tunnels are responsible for the distribution of traffic to the mobile nodes. The reverse traffic (generated by the mobile nodes) follows the paths given by the regular IP routing on the transport network.

MPA employs access subnetworks with the same network address prefix, usually in the private range. This means that the mobile nodes keep their IP addresses during handover. The wireless network is based on IEEE 802.11b/g configured with WPA2 (Wireless Protected Access 2) security employing PSK (Pre-Shared Key) or RADIUS (Remote Authentication Dial In User Service) authentication.

In MPA, the L3 addressing functions rely on the DHCP protocol. On IPv4 networks, DHCPv4 supplies network prefix, IP address, and default router. On IPv6 networks, DHCPv6 does not supply network prefix and default router, a task left to the Neighbor Discovery (ND) protocol. ND causes long delays during handover as the mobile node must wait for ND Router Advertisement (RA) messages. There are two possible solutions for this shortcoming. The access router may send RA at a higher rate, or RA messages may be synchronized with node attachments. MPA implementation for IPv6 uses the latter approach.

MPA implements a location function on the access points via L2 triggers. An L2 trigger is a notification generated when a mobile node attaches or detaches to/from an access point. The trigger is targeted to the RSVP-TE daemon running on the access router where the access point is connected to. Upon receiving the notification, the RSVP-TE daemon starts the mobile routing function.

Mobile routing in MPA employs an opaque RSVP-TE object carried on RESV (reservation) messages, the location object as shown in Fig. 2. In RSVP-TE, RESV messages are employed to refresh the soft state tunnels signaled with PATH messages. RESV messages follow the tunnel bottom-up, being processed by the routers along the path. The proposed networking architecture employs RESV messages for both refreshing

the tunnels and signaling mobile node attachments. A RESV message carrying a location object is generated as soon as the RSVP-TE daemon receives an L2 trigger notification. The location object carries a flag, the identification (MAC address) of the mobile node, its L3 (IP) address, and other information coded on TLVs (Type-Length-Value).

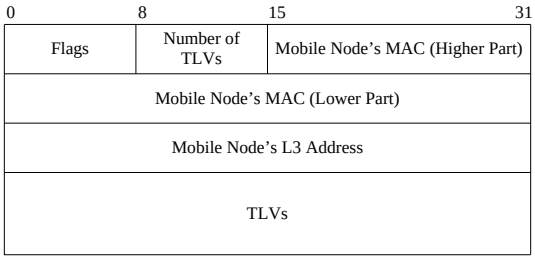


Fig. 2. The format of the RSVP-TE attachment object.

Fig. 3 shows an overlay network composed of a P2MP tunnel rooted on router R1. A mobile node is attached initially on an access point (not shown) connected to router R4. When the mobile node moves to a link served by R5, the route related to this node on the mobile routing table at R2 must be updated with a different tunnel segment (in this case from segment C to D). If the mobile node roams to a link served by R7, the mobile routing table at R1 and R3 must be updated. Updating on routing tables are performed as soon as the RESV message indicating the new point of attachment is processed by the routers.

When a mobile node disconnects, the disassociated access point generates an L2 trigger identifying the disconnection. Upon receiving this notification, the RSVP-TE daemon at the access router generates a RESV message with a location object, but with a flag indicating disconnection. The processing of this message causes the removal of routes installed for this mobile node.

MPA supports micro-mobility, that is, mobility inside a potentially large domain. For mobility across domains (macro-mobility), MIPv6 [Johnson et al. 2004] can be employed as described in [Ku and Cheng 2007].

2.1. Quality of Service

Quality of service (QoS) consists of a set of control and management functions that allows the network to guarantee some end-to-end metrics such as delay and jitter for the traffic flows generated by the applications. QoS assumes resource reservation for a particular flow, an idea in line with the Integrated Service Architecture (IntServ) [Braden et al. 1994]. IntServ relies on RSVP for signaling resource reservation along a flow path. As we employ RSVP-TE in our architecture, resource reservation may be employed. Unfortunately, the management of resources in a per-flow basis is unfeasible for small-sized routers due to the processing power it demands. In addition, QoS demands that all routers on the transport network support RSVP-TE.

A simpler approach to QoS is traffic priorization where the network establishes relative priorities for the flows, without reserving resources for each particular flow. For example, a robotic application can state that telemetry flows must have higher priority than audio and video flows. Classes of service (CoS), as defined by the Differentiated Services

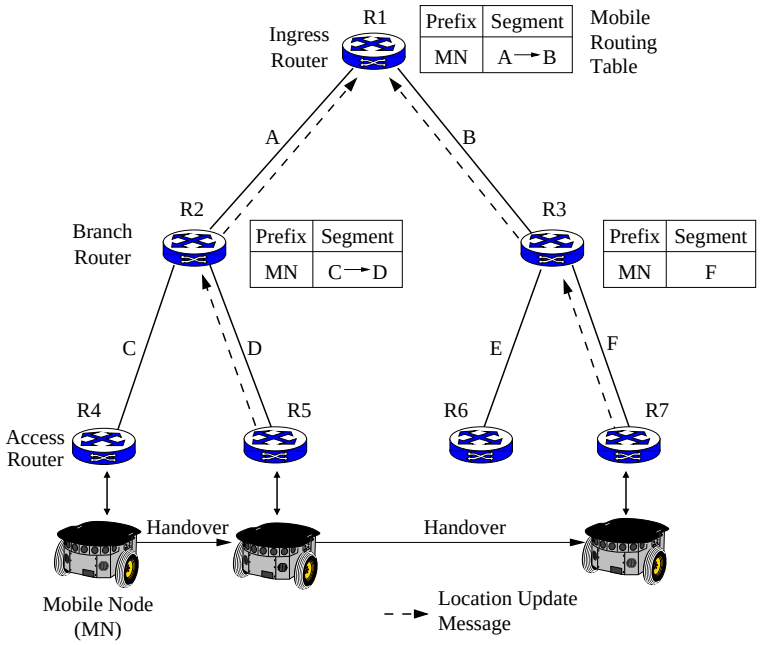


Fig. 3. Mobile routing process in MPA. Dashed arrows indicate the path of RSVP-TE RESV messages carrying location objects.

(DiffServ) Architecture [Blake et al.], represent a more feasible solution. DiffServ relies on packet markings and filters for traffic priorization on the routers along the flow path.

We implemented a combination of IntServ and DiffServ in MPA as described in the sequence. When the P2MP tunnel is created, the management application signals the RSVP-TE daemon with a set of traffic parameters necessary to build a SENDER_TSPEC [J. Wroclawski 1997] object. These parameters are, mainly, a token bucket rate and size, and a peak data rate. The Path message is signaled with this object. Each router along the path creates three queues for the traffic assigned to the tunnel based on this information. The high priority queue has 60% of the bandwidth state by the token bucket rate, the medium priority queue has 30% of the bandwidth, and the low priority queue has 10% of the bandwidth. These queues establish three classes of service (gold, silver, bronze). The queues are removed when the P2MP tunnel is dropped.

Once a mobile node attaches, the access router consults a Resource Broker to ckeck if the node has some privileges in terms of traffic differentiation. If the case, the Resource Broker returns a list of triples (Protocol, Port, Class of Service). Each triple states a priorization for a given flow produced or consumed by the mobile node. In mobile robotics applications, the following flows are common:

- media flows: video and audio flows generated or consumed by cameras, microphones, and speakers positioned on the robot;
- telemetry flows: produced by the sensoring devices present in the robot such as laser and sonar rangefinders, GPS, compass, gyroscope, encoders, etc.
- control flows: flows sent to the robot for control purposes (e.g., teleoperation).

Each flow is described by a TLV on the node attachment object (Fig. 2). The format of the TLV is shown in Fig. 4. The class of service states a priority (1 for gold, 2 for silver, 3 for bronze). The processing of the node attachment object consists in

installing packet filters on the router's core that redirects the flow to the corresponding queue according to class of service stated on the TLV. Two filters are installed in order to prioritize the flow in both directions. One filter matches packets targeted to the mobile node's port stated on the TLV. The second filter matches packets originated at the mobile node from the same port. As such, the incoming and outgoing flows to/from that port receive the same class of service.

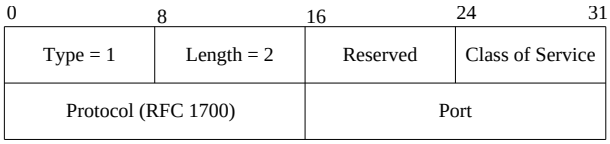


Fig. 4. Class of service TLV carried on the RSVP-TE node attachment object.

In addition to packet filters, a router processing a node attachment object with flow TLVs installs static routes for the mobile node. These static routes force the flows generated by the mobile node to follow the same tunnel route, but in reverse (upstream) direction. As such, the upstream flows cross the same routers as the downstream flows, being subjected to the same traffic differentiation thanks to the filter acting over the upstream flow. Mobile nodes without traffic differentiation have their upstream flows routed hop-by-hop. Fig. 5 illustrates the traffic differentiation procedure adopted by MPA.

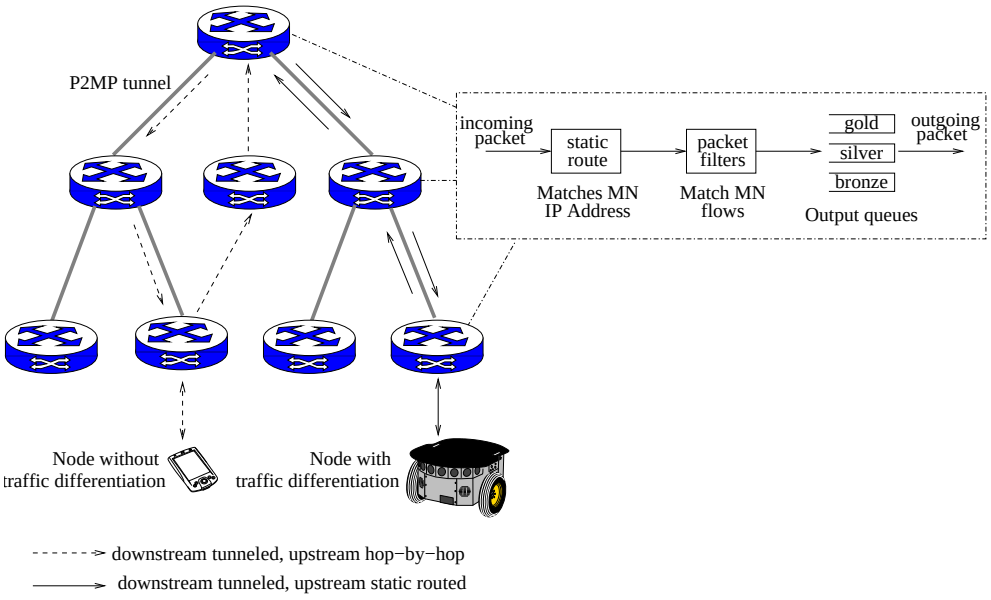


Fig. 5. Traffic differentiation in MPA.

2.2. Secure Access

In MPA the access points can be configured to authenticate mobile nodes based on WPA2 employing pre-shared keys (PSK) or RADIUS. PSK is easy to configure but is not as secure as RADIUS-based authentication. RADIUS authentication can be strengthed by using certificates installed on the mobile nodes.

As RADIUS transactions take long time (500ms in our testbed network), RADIUS-based authentication increases considerably the handover overhead. In order

to speed up RADIUS-based authentication, a cache mechanism can be employed such as PMK (Pairwise Master Key) caching (also called proactive key caching). In this mechanism, once a mobile node completes successfully a RADIUS transaction, the access point stores the PMK supplied by the RADIUS server in the cache. When the mobile node connects to a new access point, the access point queries the cache (using the mobile node's MAC address as a search key) in order to recover the PMK assigned to the node. If an entry is found, the access point accepts the mobile node without the need of a RADIUS transaction. In this case, the PMK found on cache is used to secure the communication between the mobile node and the access point. Cache entries are refreshed at each query are removed by aging (e.g., one hour without refreshing).

PMK caching can rely on a centralized or distributed databases where the access points store the PMKs assigned to the mobile nodes that successfully authenticated on the authentication server. When a mobile node switches among access points, it presents to the new access point its PMK obtained on the previous one. The new access point consults the server and, if the PMK is valid, the access point accepts the mobile node without the need of server-based authentication.

3. Implementation Details

MPA was implemented for Linux routers with extensions for IP/IP (IP over IP) tunnels and MPLS tunnels. The IP/IP extension was ported to the MikroTik [MikroTik Routers & Wireless 2008] RoutingBOARD 133 running OpenWRT [OpenWRT Project 2008], a Linux-based operating system for network appliances. The MikroTik boxes act as both router and access point. The MPA implementation consists of a RSVP-TE daemon with P2MP extensions written in C and a management front-end written in Java [Feliciano et al. 2007]. The RSVP-TE daemon was cross-compiled for the MikroTik boxes. The management front-end runs on a PC-based management station.

The management front-end interacts with the RSVP-TE daemon in order to manage P2MP tunnels. This interaction is based on the exchanging of XML messages over TCP (Transfer Control Protocol). The tool offers a menu bar with options for loading the physical network topology, discovering the logical topology of the network by polling the MPA routers for established tunnels, and managing (create, destroy, reroute, and monitor) P2MP tunnels. The front-end can run as a desktop application or as a Java applet on web browsers.

The traffic differentiation scheme was implemented above *tc*, the Linux traffic control utility. Each P2MP tunnel creates three queues with token bucket discipline. Filters for prioritizing traffic for the mobile nodes are also installed with *tc*. U32 masks are employed for matching the transport protocol, port, and origin/destination IP address (or any combination of these).

We implemented a PMK caching mechanism in order to speed up the RADIUS-based authentication. The details about this mechanism are outside of the scope of this paper.

3.1. Results from Testbed

The testbed network consists of four MikroTik RouterBOARD 133, one acting as ingress, one as branch, and two as egress routers (Fig. 6). These routers were linked through two plain Linux routers emulating an existing networking infrastructure with capacity enough to route efficiently the traffic from the MikroTik routers. RSVP-TE was installed on the MikroTik routers. The Linux routers were configured with static routes. The egress routers act also as access points configured with WPA-PSK.

The network services consist of a DHCP server from the Internet Software Consortium (ISC), a RADIUS server from the FreeRADIUS project, and an HTTP (Hypertext Transfer Protocol) server from the Apache Software Foundation. These servers run on a DELL PowerEdge 1900 server machine connected on the MikroTik ingress router. Fig. 6 shows the physical and logical (overlay) topology of the testbed network.

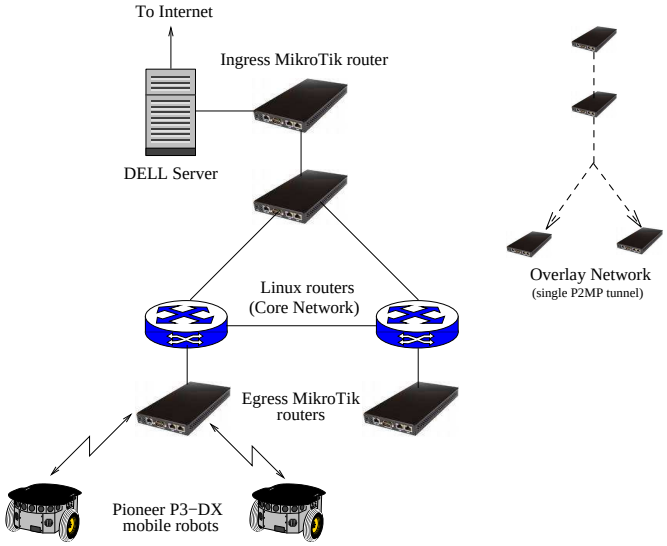


Fig. 6. Topology of the testbed network. MPA's P2MP tunnels are established among the MikroTik routers through the "core" network.

The mobile nodes are two Pioneer P3-DX mobile robots with on-board processors running Linux (Debian and Xubuntu distributions). Each robot is fitted with two on-board cameras and a sonar ring with 16 sonars. One robot is fitted with a laser rangefinder and a front gripper.

With this testbed network, measurements of handover overheads and traffic differentiation overheads (times to set up static routes and packet filters) were obtained in order to feed the simulation model. In this testbed, a mobile robotic application was running in order to assess the architecture in practice.

3.2. Results from Simulation

A simulation model from MPA described in [Johnson et al. 2008] was tuned with the parameters obtained from the MikroTik-based testbed network with mobile nodes running Linux. The simulation employs a queueing network model shown in Fig. 7. The model establishes a number of service queues that simulate the MPA operations related to node attachments.

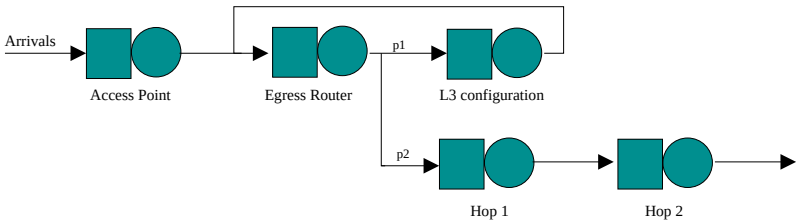


Fig. 7. Queueing network model for MPA node attachment procedures.

The objective of the simulation was to obtain the average throughput as the handover rate completed successfully as a function of two parameters. The first parameter is the size of the network given by number of routers (hops) between the ingress and egress routers. The second parameter is arrival rate of mobile nodes (number of handovers requested per second), up to 2 handovers/s. Fig. 8 shows that the proposed architecture scales appropriately for larger network topologies and mobile node dynamics (arrival rate) than employed on our testbed network.

A second simulation result is the overhead imposed by MPA as a function of the network size (number of hops between the ingress and the egress routers) and node arrival rate. Fig. 9 shows the MPA response time. The 100ms estimated for one hop, obtained from the testbed network, is coherent with the simulation model. The simulation results show that the proposed mobility architecture scales fairly for larger network environments.

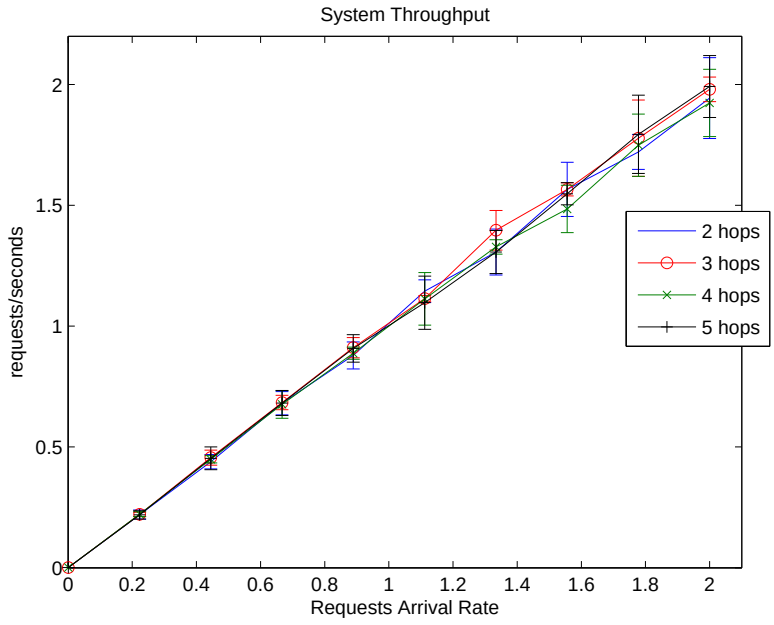


Fig. 8. Throughput of MPA running on MikroTik boxes as a function of network size (hops) and node arrival rate.

Another series of simulations were conducted in order to measure the impact of traffic differentiation on the handover overhead. Handover throughput and delay were computed as a function of the average number of flows established by the mobile nodes, ranging from zero to three. Figs. 10 and 11 show the results.

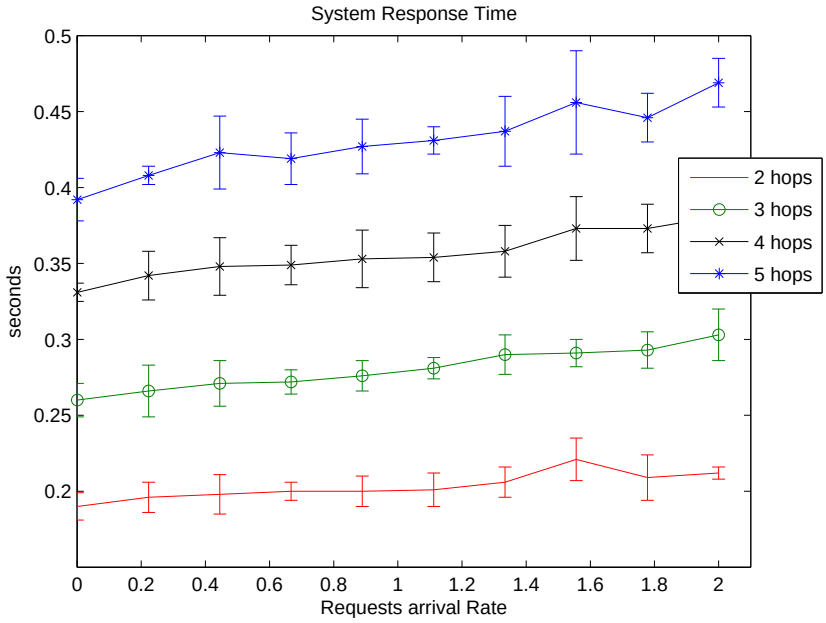


Fig. 9. Delay imposed by MPA as a function of network size (hops) and node arrival rate.

Fig. 10 shows that the number of flows does not impact on the handover throughput, the same result observed for the size of network (Fig. 8). In other words, the architecture has no bottlenecks regarding the number of flows prioritized per mobile node. In terms of handover delay, Fig. 11 shows that each additional flow introduces a handover delay of about 150ms. This overhead is debted to the installation of reverse route for the mobile node's upstream traffic and one packet filter per each flow direction. Fig. 11 suggests that the overhead increases with the arrival rate and number of flows.

4. A Network Robotics Application

A mobile robotics WebLab (REALab) developed by the authors and reported in [Coelho et al. 2007a, Coelho et al. 2007b, Moraes et al. 2009] was employed to evaluate from the user's standpoint the proposed network architecture. WebLabs allow laboratorial equipments to be operated in real time from remote sites through the public Internet or private high speed networks. The WebLab operates four Pioneer P3-DX with different configurations, high quality network cameras, and a set of servers. Mobile robotic experiments can run on the server or on the user's computer.

The REALab WebLab offers a set of mobile robotics experiments as well as allows the user to upload his/her own experiments. A group of users can access the WebLab from different locations. For groups, a token-based access control to the equipments is provided. During the execution of a remote experiment, group members communicate with the aid of a chat provided by the WebLab or by employing conference tools such as Skype and Google Talk.

By design, REALab employs the REST (Representational State Transfer) interaction style where the robot is seen as a statefull Web resource accessed via HTTP GET and POST operations. HTTP messages carry XML documents with commands to

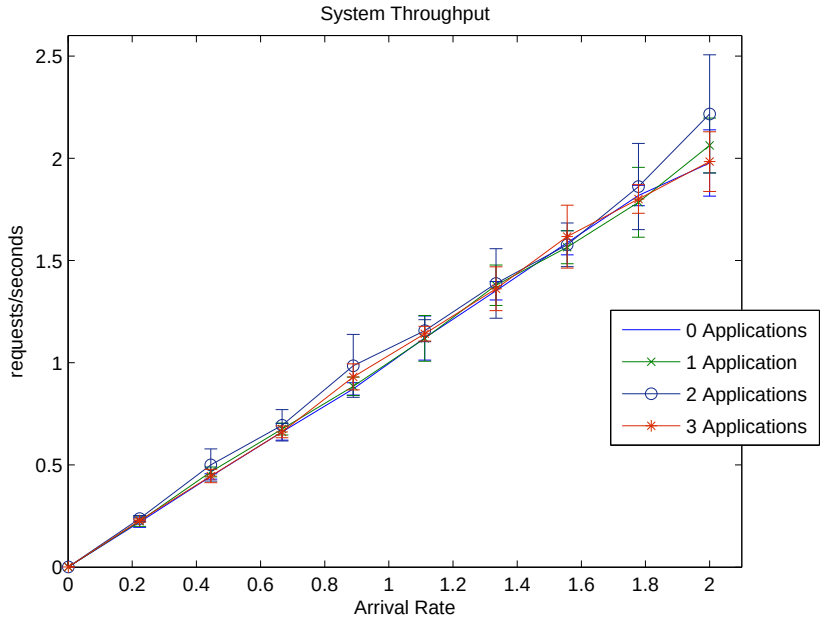


Fig. 10. Throughput of MPA running on MikroTik boxes as a function of average number of flows per node and node arrival rate.

the robot and telemetry data from the robot. Video and audio flows are transferred through RTP (Real Time Protocol) tunneled on HTTP messages.

In this paper we are interested in evaluate the traffic differentiation capabilities of MPA. Two WebLab experiments were conducted simultaneously: teleoperation and laser-based autonomous navigation. Each experiment acts over one robot and the two robots are connected to the same access router. The area where the robots navigate is small enough to avoid handovers.

Each robot produces two video flows and one telemetry flow, all over HTTP. We run the experiments with two traffic priorization configuration. In one configuration, video flows receive gold service and telemetry flows receive bronze service. In the second configuration occurs the opposite. The P2MP tunnel established (see Fig. 6) has 1.0 Mbit/s of reserved bandwidth.

As expected, when video flows have higher priority, the teleoperation experiment presents high quality video to the operator, but the operator perceives a delay when controlling the robot. In autonomous navigation, the robot follows an erratic trajectory as the control program running at the operator's station can not sustain a telemetry flow with the needed bandwidth. In the second configuration, the robot navigation is improved, but video quality drops.

Fig. 12(a) illustrates the trajectory of the robot navigating autonomously with telemetry and control receiving the bronze class of service. Fig. 12(b) illustrates the trajectory of the robot with control and telemetry receiving gold service. The quality of the trajectory (length and smoothness) clearly shows the effects of traffic differentiation over this robotic application.

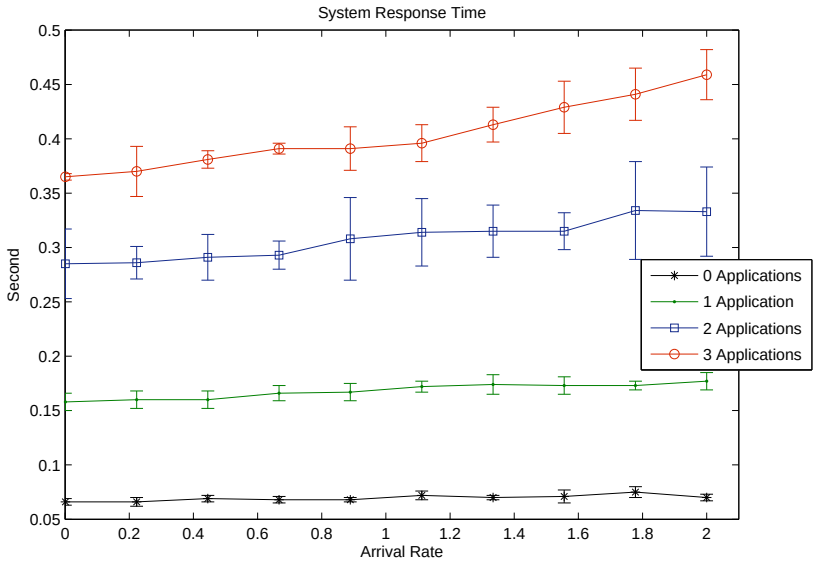


Fig. 11. Delay imposed by MPA as a function of average number of flows and node arrival rate.

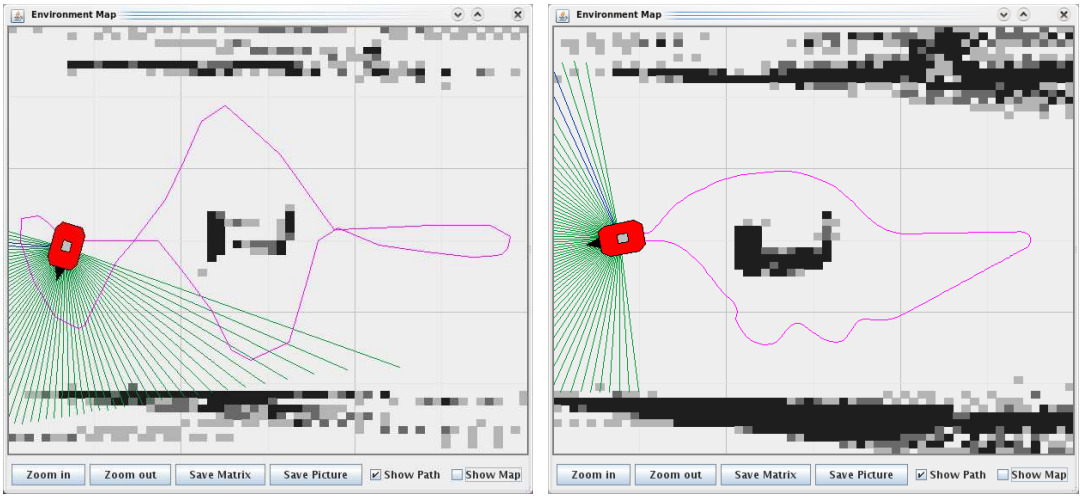
5. Conclusions and Related Work

Mobile robotics applications demand network solutions that provide secure and reliable communication with the robots independently of their current location. This paper described a network architecture that takes advantage of the existing indoor network deployments. An overlay network built with low cost access points running OpenWRT is the key element of the architecture. The overlay network addresses mobility, security, and class/quality of service, the major requirements of mobile robotics applications. The architecture demands no specialized software on the mobile robots, a key point for small mobile apparatus with reduced processing power.

The architecture relies on a combination of IntServ (RSVP-TE) and DiffServ to offer traffic priorization. For instance, control traffic can have precedence over media traffic. Also, no assumption is made about the security mechanism employed. We tested the architecture with WPA configured both with PSK and RADIUS. With RADIUS, authentication caching prevents the mobile node from performing a RADIUS transaction at each new attachment. Results from testbed and simulation show that the solutions scale fairly and can be implemented in Linux/OpenWRT-based routers without any modification or addition.

Related Work

Reference [Ku and Cheng 2007] proposes Mobile IPv6 (MIPv6) for supporting handover in network robotics environments. With MIPv6 there is no need of an overlay network (as proposed by this paper) as this protocol tolerates changes in layer 3 parameters such as network prefix and default router. This advantage, however, is shadowed by the disadvantages of MIPv6. Firstly, we can not see in a near future the deployment of IPv6 networks. Secondly, MIPv6 demands the installation of this protocol on the mobile robots. As these equipments usually lack of processing power, MIPv6 becomes unfeasible in many situations. Finally, the handover delays observed (around four



(a) (b)

Fig. 12. Potential fields trajectories with low (a) and high (b) control and telemetry priorities.

seconds) is unacceptable for many robotics applications (e.g., teleoperation). This delay is caused by the autoconfiguration process as employed in MIPv6. Surelly, the use of MIPv6 extensions such as FMIPv6 (Fast Handover MIPv6) or HMIPv6 (Hierarchical MIPv6) would improve handover overheads. Unfortunately, HMIPv6 and FMIPv6 implementations are not readily available as MIPv6.

Our solution places the mobility functions on the network, not on the mobile nodes. As such, mobile robots with very limited processing power can receive the same network service as the more equipped ones. Moreover, the native triggering process reduces handover delays to fraction of second, a figure much more realistic for network robotics applications. Reference [Ku and Cheng 2007] does not address security or quality/class of service as our solution does.

As network robotics is a new area of research we found no additional work that addresses mobility architectures in this field.

Acknowledgment

The authors at the University of Campinas would like to thank Ericsson Telecommunications of Brazil and Fapesp for supporting this research. Thanks also to Fernando P. Neto, Alessandro Moretti, and Victor V. Pinto for helping the implementation of the REALab WebLab.

Referências

Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and Swallow, G. (2001). RSVP-TE: Extensions to RSVP for LSP Tunnels. RFC 3209, The Internet Engineering Task Force (IETF).

Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and Weiss, W. Technical report.

Braden, R., Clark, D., and Shenker, S. (1994). Integrated services in the internet architecture: an overview. RFC 1633, The Internet Engineering Task Force (IETF).

Coelho, P., Sassi, R., Guimarães, E., Cardozo, E., Faina, L., and Lima, A. (2007a). Arquitetura e Requisitos de Rede para Weblabs. In *Simpósio Brasileiro de Redes de Computadores - SBRC 2007*, Belem, PA.

Coelho, P. R., Sassi, R. F., Cardozo, E., Guimarães, E., Faina, L. F., Pinto, R. P., and Lima, A. Z. (2007b). A Web Lab for Mobile Robotics Education. In *IEEE International Conference on Robotics and Automation - ICRA'07*, Rome, Italy.

Feliciano, G., Berenguel, A., Zagari, E., and Cardozo, E. (2007). Onix: Sistema Integrado para Gerência de Redes Sobrepostas. In *XII Workshop de Gerência e Operação de Redes e Serviços - SBRC 2007*, Belem, PA.

J. Wroclawski (1997). The use of rsvp with ietf integrated services. RFC 2210, The Internet Engineering Task Force (IETF).

Johnson, D., Perkins, C., and Arkko, J. (2004). Mobility support in IPv6. RFC 3775, The Internet Engineering Task Force (IETF).

Johnson, T., Prado, R., Zagari, E., Badan, T., Cardozo, E., and Westberg, L. (2008). Performance Analysis of a New Architecture for Mobility Support in IP Networks. In *IEEE International Wireless Communications and Mobile Computing Conference - IWCMC'08*, Crete Island, Greece.

Ku, C.-H. and Cheng, Y.-C. (2007). Remote Surveillance by Network Robot using WLAN and Mobile IPv6 techniques. In *TENCON 2007*, Tainan, Taiwan.

MikroTik Routers & Wireless (2008). http://www.mikrotik.com/.

Moraes, D. H., Coelho, P. R., Cardozo, E., Guimarães, E. G., Johnson, T. M., and Atizani, F. (2009). A Network Architecture for Large Mobile Robotics Environments. In *Second International Conference on Robot Communication and Coordination (Robocomm 2009)*, Odense, Denmark.

OpenWRT Project (2008). http://openwrt.org/.

Vatn, J.-O. (2003). An experimental study of ieee 80211b handover performance and its effect on voice traffic. http://www.it.kth.se/ vatn/research/handover-perf.pdf.

Yasukawa, S. (2006). Signaling Requirements for Point-to-Multipoint Traffic-Engineered MPLS Label Switched Paths (LSPs). RFC 4461, The Internet Engineering Task Force (IETF).

Zagari, E., Prado, R., Cardozo, E., Magalhães, M., Badan, T., Carrilho, J., Dolphine, T., Berenguel, A., Barboza, D., , Johnson, T., and Westberg, L. (2009). Design and Implementation of a Network-Centric Micro-Mobility Architecture. In *IEEE Wireless Communications and Networking Conference (WCNC 2009)*, Budapest, Hungary.

Zagari, E., Prado, R., Cardozo, E., Magalhães, M., Badan, T., Carrilho, J., Pinto, R., Berenguel, A., Barboza, D., Moraes, D., Johnson, T., and Westberg, L. (2008). MPA: a Network-Centric Architecture for Micro-Mobility Support in IP and MPLS Networks. In *IEEE Sixth Annual Conference on Communication Networks and Services Research - CNSR'08*, Halifax, Canada.