WiMetroNet—A Scalable Wireless Network for Metropolitan Transports

Manuel Ricardo, Gustavo Carneiro, Pedro Fortuna, Filipe Abrantes and Jaime Dias
INESC Porto, Faculdade de Engenharia, Universidade do Porto
{mricardo, gjc, pedro.fortuna, fla, jdias}@inescporto.pt

Abstract—This paper addresses Wireless Networks for Metropolitan Transports (WNMT), a class of moving or vehicle-to-infrastructure networks that may be used by public transportation systems to provide broadband access to their vehicles, stops, and passengers. We propose the WiMetroNet, a WNMT that is auto-configurable and scalable. It is based on a new Ad hoc routing protocol, the Wireless Metropolitan Routing Protocol (WMRP), which, coupled with data plane optimizations, was designed to be scalable to thousands of nodes.

Index Terms—private network; layer 2; wireless; large; mesh.

I. INTRODUCTION

In this paper, we address a class of moving or vehicle-to-infrastructure networks. Our particular network—the WiMetroNet—is a private network possibly owned by a consortium of companies which jointly operate public transportation vehicles such as buses, trams, and taxis. The scenario addressed consists of providing secure broadband wireless access to a few thousands of vehicles and vehicle stops. Each vehicle will use its access to operate services such as video-surveillance, video broadcast, and video/voice calls. Besides, each vehicle is expected to provide wireless access to its passengers, which carry portable and conventional equipments with standard IEEE 802.11 (WLAN) interfaces and a bare IP communications stack. Passengers may access the Internet not only from the vehicles but also from the stops while waiting for the vehicles and are allowed to communicate between themselves.

Vehicles get a broadband wireless access by using heterogeneous wireless technologies. Each vehicle has an IEEE 802.16 (WMAN) access which may not be accessible from every place, an IEEE 802.11 (WLAN) access which is used when the vehicle approaches some stops, and a 3GPP Universal Mobile Telecommunications System (UMTS) access, which it uses when uncovered by the other technologies. Each vehicle/stop is equipped with a communication equipment—the Rbridge—which manages the wireless broadband access and serves one or more WLAN Access Point (AP) located inside the vehicle/stop, to which the passenger or other vehicle equipments can associate. Figure 1 presents the WiMetroNet reference architecture. When, for instance, a passenger arrives to a tram station, he gets a secure wireless access and IP connectivity. While moving from the tram station to a tram, from the tram to the arrival station, and from there to a bus, the passenger is expected to maintain its connection and observe no considerable degradation on the quality of his communications.

The WiMetroNet is a mesh network of moving Rbridges. It is auto-configurable, and it operates at layer 2.5 over heterogeneous wireless technologies. An Ad hoc routing protocol is used, as well as secure mechanisms for authorization, authentication and confidentiality. A passenger’s equipment will see WiMetroNet as its LAN, thus being one IP hop away from the other terminals attached to WiMetroNet and from its default router. While moving, terminals maintain their IP addresses. We will refer to the class of networks similar to WiMetroNet as Wireless Network for Metropolitan Transports (WNMT).

The paper is organized as follows. Section II, WNMT traits, provides an overview of the main aspects and solutions to consider when designing this type of moving networks; we address the characteristics of the wireless technologies, possible networking strategies, mobility management solutions, security methods, and new congestion control paradigms. Section III describes the WiMetroNet network architecture. Section IV identifies the open research problems.

II. WNMT TRAITS

This section presents a discussion on technologies that can be used to design a WNMT.

A. Wireless technologies

In Table I, the main wireless technologies used to build local, metropolitan, and wide area networks are identified. UMTS is a major 3G wireless technology, which achieves wide coverage through spatial reuse of radio resources, and roaming between operators. UMTS allows fast handovers between cells, and vehicular communications up to 250 km/h. UMTS Rel99 supports peak data rates ranging from 384 kbit/s (urban outdoor) to 2048 kbit/s (indoor and low range outdoor). HSDPA (Rel5) can provide data rates up to 14.4 Mbit/s, with a latency of about 70 ms.

The IEEE 802.16 technology addresses the WMAN. Using the line of sight transmission band (10-66 GHz), an 802.16 cell can have a radius of 50 km, with a maximum data rate of 75 Mbit/s. It is used to offer access to Subscribers Stations or as a back-haul network. The IEEE 802.16a amendment enables the use of non line of sight transmissions. In addition to the
single-hop point-to-multipoint operation, 802.16a specifies the support for mesh networks. The 802.16e amendment adds mobility support, providing support for handoffs to stations moving up to vehicular speeds. The real 802.16e performance is considerably less [1] than the theoretical limits, with total bandwidth per Base Station (BS) averaging a few Mbit/s or less, and performance decreasing considerably for distances above 1 km.

The IEEE 802.11 WLAN offers coverage of up to 100 m outdoor and 30 m indoor, in unlicensed bands. The 802.11b/g works on the 2.4 GHz ISM band, while 802.11a uses the 5 GHz U-NII band. The maximum data rates are 11 Mbit/s for 802.11b, and 54 Mbit/s for 802.11a/g. The 802.11s standard enables these networks to work in mesh modes.

New radio techniques are expected to enable higher data rates for these technologies. 802.16m 100 Mbit/s and 1 Gbit/s for mobile and fixed stations, respectively, and the UMTS High Speed OFDM Packet Access will provide up to 100 Mbit/s.

In WNMTs, there is no single link layer technology satisfying all their needs, and multiple technologies shall be combined. For connecting users’ equipments to a vehicle, for instance, 802.11 is preferred due to its good performance and availability in terminals. On the other hand, 802.11 is generally not adequate to connect vehicles to the infrastructure due to its very short range and low maximum supported speed. For this purpose, technologies such as mobile 802.16 and UMTS are better suited. Between 802.16 and UMTS the choice is not trivial, but deciding factors may include network deployment costs, traffic costs, and the strategic requirement of some transport operators controlling their entire network.

B. Networking

Packet networks can be classified into packet switching and virtual circuit (VC) switching. A switch of the first type forwards a packet based on its final destination address; a switch of the second type forwards a packet based on a label carried by the packet which identifies the circuit.

In order to forward a packet based on its destination address, each switch has to look up a forwarding table. Each entry of this table associates a destination address to an output port. Technologies such as 802.1D behave in this way and, since they use unstructured 48 bit MAC addresses, their forwarding tables contain one entry for each known address. Some other network technologies, such as IP, may use structured addresses; in this case, an entry of the table contains forwarding information for an entire sub-network. Structured addresses lead to shorter forwarding tables and lookup times than unstructured addresses; they also enable the deployment of large networks, because entries in the forwarding tables can be organized using techniques such as classless IP addresses. However, structured addresses preclude network auto-configuration because they have to be engineered and configured manually.

A VC is commonly interpreted as a path along the network which must be established before packet transmission. This path may be characterized by a single identifier, with global significance, or by a sequence of identifiers (labels), each having local significance between adjacent switches. When a switch receives a packet, it looks up its forwarding table. An entry of this table contains information about the output port and about the label that will be used by the packet on the next segment of the path. Thus, from switch to switch the packet sees its label substituted. Technologies such as the Multi-protocol Label Switching (MPLS) use labels as identifiers.

Some other networking technologies, such as tunnels, Transparent Interconnection of Lots of Links (TRILL), IP source routing, MPLS based VPNs, or 802.11s, use layered approaches, where packet switching and VC switching may be combined. In these cases, paths are defined based on MAC.
addresses, IP addresses, or MPLS labels. The 802.11s packet, for instance, contains 4 MAC addresses: source and destination stations, and the addresses of the mesh points attached to the current segment of the path. When an 802.11s mesh point receives a packet it looks up its forwarding table using the packet destination address; an entry of this table contains the MAC address of the switch to which the packet must be forwarded, which is used to re-arrange the MAC addresses of the packet before it is forwarded.

The existence of a Time To Live (TTL) field is intimately connected to the support of mesh topologies. Technologies such as MPLS and IP have a TTL and support mesh topologies, while 802.1D has no TTL and does not support mesh topologies.

Candidate solutions for WNMTs should contain the following ingredients: scale to thousands of nodes, support mesh topologies, support mobility, and be auto-configurable. None of the technologies in Table II fulfills all of these requirements. While 802.1D is auto-configurable, it does not scale to a WNMT size, mainly due to the way it handles broadcasts [2], and does not support mesh topologies. TRILL adds a TTL and link state routing to 802.1D networks, allowing it to support mesh networking, but it improves little on the scalability of 802.1D, and does not support mobility. 802.11s supports mobility and mesh networking, but it has very limited scalability. IP and MPLS are both scalable to a WNMT size and support mesh topologies, but their control planes require manual configuration. However, their data planes can be useful.

### C. Mobility management

There are two major classes of mobility management. Terminal mobility enables terminals to change point of attachment without user intervention, while network mobility addresses the movement of intermediate nodes.

Table III summarizes the properties of terminal mobility solutions. Mobile IP [3], for instance, is an IP (L3) mobility solution, works regardless of the link layer technology, and makes mobility transparent to TCP/UDP and applications. Mobility solutions implemented at the link layer level, such as in UMTS networks, allow the terminal to switch Point of Attachment (PoA) transparently to the IP layer, i.e. the IP address of terminal never changes. The Host Identity Protocol (HIP), on the other hand, operates at layer 3.5, and so it is able to provide mobility support on top of either IPv4 or IPv6 transparently to TCP or UDP based applications. The Session Initiation Protocol (SIP) supports mobility at the “session layer” (L5) of the OSI stack. In general, a mobility solution requires that the location of the mobile terminal is tracked by an agent, and routes for packet delivery be rebuilt in real time.

Mobility solutions can also be classified by their geographical scope. Global mobility solutions, such as Mobile IP (MIP) or HIP, support any kind of mobility. Local mobility solutions, on the other hand, only support transparent mobility within a certain network domain, as is the case of eTIMIP [4], or Proxy MIP [5]. Access technologies, such as 802.16 or 802.11, support only local mobility. Global scope mobility protocols ensure that mobile nodes are always reachable, but they have poor performance because the mobility agent is located far from the moving terminals. Local scope mobility is more efficient but only achieves mobility transparency within a limited network region. Mobility solutions are also characterized by the set of nodes requiring modifications. Solutions such as MIP or HIP require modifications in the terminal. Solutions like Proxy MIP are implemented by the network, and require no modification in the terminals.

Network mobility solutions allow some intermediate nodes to change PoA without disrupting the ongoing data sessions. In normal IP networks, when an access router changes PoA it must change the IP address of one network interface. However, intra-domain routing protocols like Open Shortest Path First (OSPF) usually take tens of seconds to detect topology changes and to install new routing tables in the remaining routers of the access network; during this time packets get lost. The NEMO protocol optimizes this scenario by extending the MIP approach to *mobile routers*.

Ad hoc networks appeared as a new communication paradigm in which nodes spontaneously form networks in mesh-like topologies. Traditional routing protocols were found inadequate, since they assume some kind of structured organization of the network, i.e. division of the network into routing areas. Ad hoc routing protocols such as Ad hoc On-Demand Distance Vector (AODV) and Optimized Link State Routing (OLSR) were defined. The former is a reactive Ad hoc routing protocol in which routes are discovered only when
packets need to be transferred; the latter is a proactive solution, where routes are periodically disseminated via flooding of link state packets containing each node’s list of neighbors, and permanently maintained. Ad hoc routing protocols can be tuned for mobile scenarios by forcing the discovered routes to expire very quickly, in case of reactive protocols, or by having a very short route flooding interval, in the case of proactive protocols.

In WNMTs, the need for a solution with a great degree of auto-configuration implies the use of Ad hoc networking. However, existing Ad hoc routing protocols were designed for networks with a few dozen nodes, and will not scale to thousands of nodes. In addition, their support for terminal or router mobility is inefficient, allowing several seconds to pass before node movement is properly detected by the network. Possible solutions for WNMTs, in addition to solving these problems, should incorporate mechanisms allowing the network to manage mobility on behalf of the terminals, as exemplified by Proxy MIP and eTIMIP.

D. Security

The main pillar of a wireless security framework is the authentication, without which it is not possible to deploy access control, integrity or confidentiality. A BS needs to authenticate stations prior to decide if they are allowed to access the network. The simplest authentication method uses pre-shared keys. While this works for a personal or small network, it does not scale for large networks. When the number of users grows the best approach is to configure the access points to delegate the tasks of authentication and authorization to a central Authentication Server (AS). An Authentication, Authorization, Accounting protocol such as RADIUS, may be used for that purpose. This approach allows the deployment of BSs with simple logic, and facilitates the management of the user’s credentials and of the access control lists.

Each wireless technology includes its own security mechanisms. In UMTS the subscriber has a token, an Universal Subscriber Identity Module (USIM) containing a secret key. This key is used to authenticate the user in the network and to derive a key used to encrypt data between the terminal and the BS. The authentication is processed centrally by the Authentication Center (AuC). 802.16e specifies two authentication mechanisms: PKM RSA, which uses X.509 certificates to bind public RSA encryption keys to the MAC addresses of the stations; and PKM EAP, which is used in conjunction with an Extensible Authentication Protocol (EAP). The 802.11i amendment to the 802.11 standard defines two authentication modes: one with pre-shared keys and another with an AS. The latter mode uses 802.1X, a generic access control protocol for IEEE 802 networks which can be used together with EAP. The EAP enables users to be authenticated using the same methods in different L2 networks, including UMTS via the EAP-AKA method, in addition to 802 networks.

In order to scale to a WNMT, security mechanisms require a centralized AS which allows BSs to be simple and auto-configurable, have simple management of credentials and access control lists and, together with EAP, flexibility in the authentication. However, the authentication process is the major contributor for the delay during a station handover. In 802.11i, for instance, the authentication may last seconds, which brings problems for real-time applications. Pre-authentication and fast reconnect mechanisms should be used whenever possible in order to eliminate or mitigate these problems.

E. Congestion Control

End-to-end congestion control is a distributed task performed mainly by the end-hosts through the algorithms embedded in TCP. TCP has some undesirable properties such as increased queuing delay, unstable throughput, Round Trip Time (RTT) dependent fairness, and inefficiency for high bandwidth delay product networks or high error-rate networks. The limitations of TCP result from the fact that it relies on low resolution feedback signals of congestion from the network, such as packet drops or Explicit Congestion Notification (ECN) marking, leaving too much guessing to be done.
by TCP in choosing the sending rate, and explains why it fails to maintain a stable and accurate throughput. Alternative approaches to the congestion control problem include using feedback signals to the source other than packet drop or marking, such as the RTT delay [6], or using explicit quantitative feedback from routers [7]. Both signals have multi-bit resolution, allowing the congestion control algorithms to have a more stable and fair distribution of networks resources by the flows demanding them. The performance of explicit congestion control seems particularly promising in WNMTs.

Heterogeneous wireless mesh networks, in part due to the high variability of RTTs, in addition to the low capacity of wireless link, are especially prone to congestion, which has a considerable impact on delays and requires large buffers in core Rbridges. Modern congestion control schemes, deployed in Rbridges, would contribute to maintain low network queuing delays and high degree of fairness.

III. THE WIMETRONET NETWORK ARCHITECTURE

The WiMetroNet network, exemplified in Figure 1, is generally structured in the following way. There are Rbridges in vehicles and bus stops or tram stations. They provide 802.11 connectivity to some vehicle equipments and to the users’ terminals. Vehicles connect to the network core Rbridges through 802.16e, while moving, or through 802.11 to the bus or tram stops Rbridges’, while stationed near them; the Rbridges in bus stops or metro stations are connected to the core via high speed wired links, where possible, or fixed 802.16a wireless connections, for the most remote locations. At the WiMetroNet core a number of Rbridges are deployed in a Gigabit Ethernet mesh topology, and the WiMetroNet control plane ensures that optimum paths are used for forwarding traffic between different edge Rbridges. Finally, there is at least one IP router functioning as Internet gateway.

The terminals connect to one of the edge Rbridges, acquire an IP address through DHCP (the DHCP broadcast requests are tunneled to a well known DHCP server). The user traffic is then encapsulated when entering the WiMetroNet network, transported inside the network, and the original frames delivered to the destination station, or to the Internet gateway. Following the scalability principles outlined in Section II-B, in WiMetroNet broadcasts are strictly controlled and special algorithms and optimizations have to be employed for ARP, Neighbor Discovery, DHCP(v6), and generic service discovery.

Unlike L3 Ad hoc networks, which use routing protocols such as OLSR and AODV, the WiMetroNet architecture does not require terminals to run any kind of special protocol, routing or otherwise; only the standard 802.11 family of protocols. On the other hand, full support for mesh topologies is required in order to maximize the wireless network capacity. This leads to the need for a TTL field. However, the frame headers of IEEE 802 access technologies do not contain a TTL field. The WiMetroNet architecture solves this problem by introducing of a new L2.5 header containing a TTL. This new header should be small to avoid excessive overhead, which led to the adoption of the standard MPLS header for WiMetroNet data plane. On top of the MPLS layer the original L2 frame is encapsulated.

As an example, consider one terminal, traveling inside a bus, that is interacting with an HTTP server outside WiMetroNet. Suppose also that the bus is temporarily stationed at a bus stop, and so the WiMetroNet control plane has selected an optimized route to reach the Internet that goes through the 802.11 link between the bus and the bus stop, via an AP, then 802.3 (e.g. Gigabit Ethernet) from the bus stop to the network core, and finally 802.3 to the Internet gateway, as shown in Figure 2. As the user traffic arrives at an edge Rbridge (inside the bus), an ingress operation takes place. Ingress includes the following steps:

1) the L2 frame is first converted to a canonical Ethernet II encapsulation, i.e. [destination MAC, source MAC, “EtherType”, payload];
2) the destination MAC address is used to lookup the egress Rbridge in a local terminal location database, which is a table mapping MAC addresses of known terminals to Rbridges. The information from this table is collected by the edge Rbridges, when they learn about attachment of terminals, and disseminated to the other Rbridges via the routing protocol;
3) knowing the egress Rbridge, the routing table is then used to lookup a label and an outgoing interface;
4) finally, the user data frame is encapsulated in an MPLS header containing the correct label and non zero TTL value, and transmitted through the outgoing interface.

When the MPLS frame arrives at an egress Rbridge it is “decapsulated” and the original user frame transmitted to the destination station.

For the control plane, WiMetroNet runs a routing protocol, the Wireless Metropolitan Routing Protocol (WMRP). It is a proactive, link state, Ad hoc routing protocol, which works directly over L2 and exchanges 20 bit identifiers instead of IP addresses. In this way, each Rbridge’s routing table instantly becomes a default MPLS forwarding table, if we consider that we have implicitly set up a default Label Switched Path (LSP) between all pairs of Rbridges, and that the outgoing label for the LSP to a given destination Rbridge is always equal to that Rbridge’s 20 bit identifier. In other words, we use a label merging technique, which has good scalability properties, as shown in [8]. In this routing protocol the location of terminals and of Rbridges is treated separately; different databases and different routing messages are employed for each one.

WMRP makes use of techniques that enable it to scale beyond the limits of traditional link state routing protocols such as OLSR or OSPF. In WMRP, the periodic link state messages are exchanged at very reduced rate of one message every 60 seconds (compare with 5 second interval of OLSR TCs). On top of this very slow refresh rate, additional mechanisms are employed to support network mobility and terminal mobility. For the case of network mobility (moving vehicles), as soon as the moving Rbridge attaches to the new (Rbridge) PoA it notifies its old PoA of its new location.
The old PoA immediately broadcasts a new link state packet, with a limited TTL such that it can reach the new PoA of the moving Rbridge. In this way only a small portion of the network is notified of the mobility immediately, but enough to get packets routed to the correct location until the next periodic flooding. For terminal mobility a slightly different approach is used. When a terminal moves, it is detected by the new PoA, which then notifies the old PoA. Afterwards a packet may arrive at the former Rbridge serving the terminal, in which case it is tunneled to the correct new location. Moreover, to prevent additional incorrectly routed packets, a binding update message indicating the new terminal location is sent to each Rbridge sending packets for this terminal at the old location. It can be shown that these three modifications to classic proactive routing protocols will achieve a low routing overhead—even considering low bandwidth (a few hundreds of kbit/s) links—and good convergence time.

One of the features of the WiMetroNet architecture is its support for heterogeneous technologies. Moreover, the same Rbridge has multiple interfaces, which are usually always active, though not all used. It is the routing protocol and its metrics that decides which interface to use at any given time. In WiMetroNet preference is given to 802.11 interfaces, then 802.16, and finally UMTS, although this ordering is configurable. When, for instance, a 802.16 link is lost a vehicle then 802.16, and finally UMTS, although this ordering is considered for low bandwidth (a few hundreds of kbit/s) links—and good convergence time.

IV. RESEARCH ISSUES

Research topics related to WiMetroNet include bootstrap, mobility, and security. With respect to bootstrap, the Rbridge 20 bit unique identifier may be obtained from a MAC address or from negotiation between Rbridges, and the performance and robustness of these approaches needs to be evaluated. Regarding terminal mobility, the solution defined in WMMP becomes temporarily reactive routing during handover. For massively peer-to-peer communications the efficiency of this approach relatively to purely proactive solutions needs to be evaluated. Additionally, the techniques used to support fast re-authentication methods, such as those being proposed by IEEE 802.11r, also have to be evaluated and improved in the context of WiMetroNet like networks. Finally, security issues include the fact that 802.11 stations are not able to distinguish APs belonging to different domains that use the same SSID, and the need to improve IEEE 802.11i in this respect.

V. CONCLUSION AND FUTURE WORK

This paper has addressed the topic of moving mesh networks working over heterogeneous wireless technologies. The topic has been discussed from the perspective of a metropolitan-scale network planned to serve a very large public transportation system and their users.

Firstly, a set of topics relevant for the design of this type of networks were surveyed, namely transmission technologies, networking strategies, mobility management, security and congestion control. Then, an overview of WiMetroNet was given. As a layer 2.5 solution, WiMetroNet becomes transparent to the terminals, who see it as their LAN. While moving in a very large region, the terminals become one IP-hop away from their default router, and use standard networking stacks including DHCP clients and ARP mechanisms.

We have also highlighted the research issues associated to the development of a large-scale unstructured mobile network, which is part of our future work.

ACKNOWLEDGEMENTS

This work is partially funded by by the Portuguese “Agência de Inovação” and the Portuguese “Fundação para a Ciência e Tecnologia”.

REFERENCES