Exploring Multi-path Communication in Hybrid Mobile Ad Hoc Networks

Roberto Speicys Cardoso, Mauro Caporuscio

Exploring Multi-path Communication in Hybrid Mobile Ad Hoc Networks

Roberto Speicys Cardoso and Mauro Caporuscio

INRIA Paris-Rocquencourt, Domaine de Voluceau-Rocquencourt
B.P. 105, 78153 Le Chesnay Cedex - France
firstname.second_name@inria.fr,
WWW home page: http://www-rocq.inria.fr/arles

Abstract. Ambient computing requires the integration of multiple mobile heterogeneous networks. Multi-path communication, in such scenarios, can provide reliability and privacy benefits. Even though the properties of multi-path routing have been already extensively studied and a number of algorithms have been proposed, implementation of such techniques can be tricky, particularly when resource-constrained nodes are connected to each other through hybrid networks with different characteristics.
In this paper we discuss the challenges involved in implementing multi-path communication on a middleware for hybrid mobile ad hoc networks. We present the PLASTIC middleware, some compelling applications of multi-path communication and the main issues concerning their implementation as a middleware-provided communication primitive.

Key words: Multi-path routing, middleware, ad hoc networks

1 Introduction

Ambient computing requires the seamless integration of heterogenous networks. Resources in an environment may be available through independent networks using different technologies, and users must be able to access them regardless of communication heterogeneity. For instance, a group of collocated resources (e.g. a printer and a projector) may be connected through a Bluetooth network while another remote resource is only accessible through WiFi (e.g. a file server). Fortunately, the convergence of multiple network interfaces into a single mobile user device can greatly simplify this task. Current cellphones featuring heterogeneous network interfaces (e.g. Wi-Fi, Bluetooth and cellular 3G) can provide users with access not only to resources on networks directly connected to the device but also by forming ad hoc networks and accessing resources on remote networks through other mobile devices.

We call these mobile networks that use heterogeneous wireless technologies *hybrid mobile ad hoc networks* (HMANETs). They are typically formed by independently managed networks connected to each other by multi-homed devices (also referred to as bridges). All nodes in such networks are potentially mobile

(as opposed to wireless mesh networks [1]) and any two nodes may be directly connected by multiple different links (in opposition to traditional mobile ad hoc networks (MANETs) where any two nodes share at most one direct connection). More importantly, those connections use different technologies and present heterogeneous properties such as delay, throughput, security, energy consumption and cost. Figure 1 shows the differences between MANETs and HMANETs.

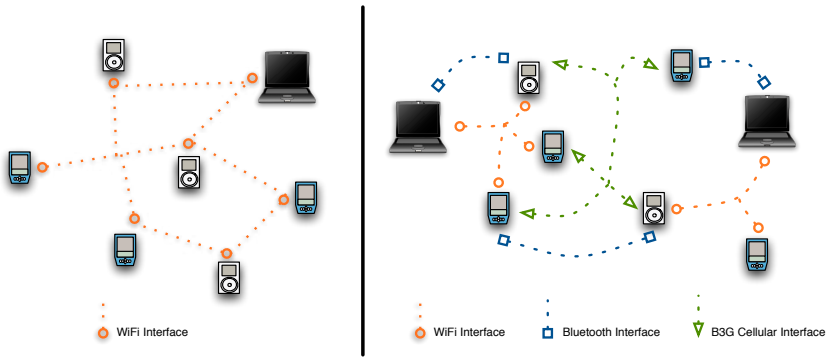

Fig. 1. A MANET and a HMANET

One consequence of the network interface diversity is that there are potentially multiple paths, with different properties, between the source and destination nodes of a message. Applications can take advantage of this path redundancy by using multiple paths for a single communication. Nodes can send the **same message** through different paths to tolerate unpredictable connection failures, which is particularly important in networks that present unstable structures. Nodes can also send **parts of a message** through different links to enhance communication privacy and resistance against eavesdropping. Messages can be divided into shares in such a way that an attacker has to control a certain number of shares to reconstruct the whole message.

However interesting the multi-path approach might be, the implementation of point-to-point multi-path communication on a hybrid mobile ad hoc network is complex. Our goal is to enable a node possessing multiple interfaces to establish a session with another node equipped with multiple interfaces regardless of the IP addresses they use to communicate; messages that belong to the same session may have different source and destination IP addresses. The Internet Protocol suite, however, does not natively support such communication through multiple paths. It is not possible, for instance, to create a single unicast TCP session that spans multiple source and destination addresses. Even when using connection-less UDP, application-layer code is necessary to determine that packets containing different source and destination IP addresses are part of the same session. Multicast can be used to send the same message to several destination

addresses through multiple paths, but it does not support sending from different source IP addresses nor sending different parts of the same message to multiple destination addresses. Additionally, the topology of a HMANET changes frequently and multi-path communication must adapt dynamically to the properties of available connections.

Such characteristics call for a middleware approach for multi-path routing. By managing multi-path routes on a layer above the network, the middleware can profit from the routing protocols already implemented and running locally on each network and create an overlay network responsible for routing packets among hybrid networks. Multi-path routing on this overlay network can take into account higher-level properties such as reliability, trust and security of nodes and networks traversed by packets. The middleware can also easily manage sessions comprising different overlay connections between nodes on hybrid networks.

In this paper we reflect on the practical challenges involved in providing multi-path communication capabilities as part of a middleware for hybrid mobile ad hoc networks. Many research efforts studied the properties of multi-path routing in MANETs [14], and proposed applications such as using multiple path routing for improving the quality of service [11] and the use of multiple routes for load balancing [16]. In this paper, however, we investigate scenarios where we are more interested in guaranteeing that a message will reach its destination reliably and privately. For this reason, we will focus on two types of multi-path communication applications: **message redundancy** to improve communication reliability and **message sharing** to improve communication privacy.

The paper is organized as follows. In Section 2 we present the PLASTIC middleware, which we will use as a case study for describing implementation issues. In Section 3 we discuss some applications of multi-path communications that are particularly compelling in HMANETs and in Section 4 we detail the issues concerning implementation of such features on the middleware layer. Finally, in Section 5 we present our conclusions and future perspectives.

2 PLASTIC Overview

The PLASTIC project aims at developing a comprehensive provisioning platform for software services deployed over B3G networks[1]. The project builds upon both Web services and standard component-based technologies and integrates methods and tools for service development, from design to validation, and a supporting middleware for service provisioning in B3G networks. In particular, the main objectives for the PLASTIC middleware are (1) allowing the deployment of services over a large diversity of terminals, including (mobile) wireless, resource-constrained ones and (2) supporting advanced functionalities for mobile adaptable services, i.e.: context-aware service management, trust and security management, SLA enforcement, and information dissemination.

Towards the first objective, the PLASTIC middleware (showed in Figure 2) builds upon the Web Service Architecture, so as to benefit from the perva-

[1] http://www.ist-plastic.org

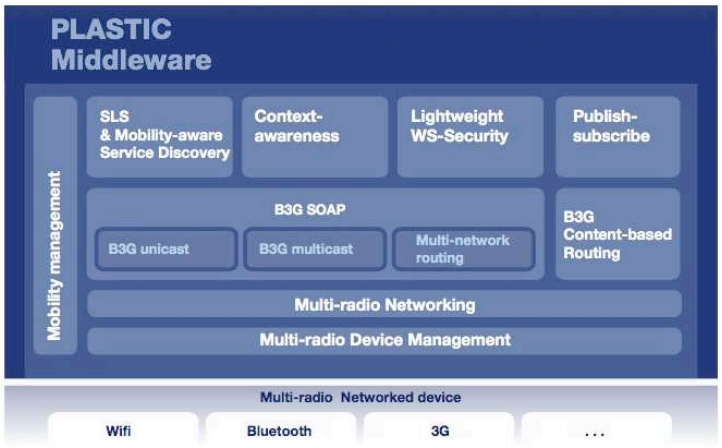

Fig. 2. PLASTIC Middleware

sive nature of Web technologies that makes them available in most digital environments (*B3G SOAP layer*). The PLASTIC middleware assumes an all-IP environment but without global routing, and enables the effective exploitation of B3G networking capabilities by composing the various networks in reach to improve availability of services and to offer seamless mobility. This specifically calls for routing protocols for the B3G network (*Multi-network routing*), where routing should meet requirements associated with both the communication protocols used at the application level and the features of the underlying composed networks (*B3G unicast* and *B3G multicast*). Also, the middleware manages the various radio interfaces (*Multi-radio Device Management*) that are embedded on wireless devices, offering the abstraction of an integrated multi-radio interface to the software services of the upper layers (*Multi-radio networking*). Such abstraction increases the quality of service access by exploiting the underlying redundancy of B3G network connectivity that results from having distinct radio network links directly connecting two nodes in a transparent way for users.

With respect to the work presented in this paper, we are interested in the Multi-radio Networking layer. Its primary role is to enable the following core functionalities: (1) PLASTIC-Address management, (2) providing communication facilities and (3) interface activation and network selection. In order to identify an application in the network, it is associated to a PLASTIC-Address, a unique identifier that resolves into the actual set of IP addresses bound to the device hosting the application. Upper layers can use this address instead of the traditional IP-based addressing scheme. The PLASTIC-Address is automatically generated and managed by the Multi-radio Networking layer. This layer also provides two types of communication facilities: (*i*) *synchronous unicast* is used to read/write packets exchanged during the interaction between client and user applications, and (*ii*) *asynchronous multicast* allows the user application to

send multicast packets to all members of a group. Finally, this layer also activates and selects the best possible networks (among those available) with respect to application- and user-required QoS level.

3 Multi-path Communication Applications

As discussed in Section 2, we assume an environment with multiple highly heterogeneous networks running the IP protocol, but without global IP routing. Devices featuring multiple network interfaces can independently form ad hoc networks and some of them may volunteer to route packets between different networks, creating an overlay network formed by bridges and heterogeneous wireless networks. This overlay network can provide various independent paths between a source and a destination, that can be explored to balance connection instability.

The goal of the multi-path communication middleware component is to improve the existing PLASTIC single path communication with multiple path routing. Multi-path communication is used autonomously by the middleware based on user-defined criteria, and exposed to applications through a middleware API. This allows applications to use reliable or privacy-preserving communication for critical messages only, reducing the performance cost of multi-path routing.

Different types of route exist on a network. According to [14], routes can be node-disjoint, that have no links or nodes in common, link-disjoint, that have no links in common and non-disjoint, that may have nodes and links in common. In HMANETs, however, we consider two different types of nodes: network nodes and bridge nodes. A route in a HMANET, then, alternates between bridge nodes and network nodes and as such we can have bridge-disjoint routes (do not have bridges in common), network-disjoint routes (do not have networks in common) and totally-disjoint routes. Even though totally-disjoint routes offer stronger reliability, network-disjoint and bridge-disjoint routes are also important. Networks on a HMANET are heterogeneous and present different levels of stability, so network-disjoint paths help to establish a more reliable communication channel. Bridges are also unstable because they are voluntary and may move or cease to work as a bridge so bridge-disjoint paths are necessary to provide alternative routes.

To improve communication reliability, the middleware uses message redundancy. The goal of message redundancy is to send the same message across different paths to increase the probability that it will reach its destination. Based on the characteristics of available routes (such as reliability, latency or throughput) the middleware must decide how many additional routes are required to achieve a certain reliability. The middleware must also dynamically determine which type of route (bridge-disjoint, network-disjoint or totally-disjoint) is necessary to obtain a reliable communication channel.

Message sharing can enhance communication confidentiality and improve privacy. The idea of message sharing is to divide a message into multiple parts that can be sent through different communication channels in such a way that, to recover the contents of a message, an attacker must control a certain number of

shares. By spreading those shares through channels with heterogeneous properties, attackers have to use more resources to access the contents of a message than in the traditional single-path communication model.

This property can be obtained through a (M, N) coding algorithm such as [2], where N is the total number of shares and M is the number of shares required to obtain the message. Coding algorithms have the advantage of causing a small overhead as each coded share is smaller than the original message. However, each share reveals something about the whole message, and an adversary controlling X messages, $X < M$, can guess the $M - X$ remaining shares and recover the whole message, which is undesirable for privacy protection.

Another possibility is to use a (t, n) secret-sharing scheme [18] where n is the total number of shares and t is the number of shares necessary to recover the whole message. Protocols such as [12] that perform multi-path routing using traditional secret sharing schemes, however, incur on an excessive overhead because in those schemes each share must be at least as big as the message itself [3]. An attractive solution is to use a scheme with computational secrecy [7] instead of a scheme with perfect secrecy. A secret sharing scheme with computational secrecy has the advantage of resulting in an overhead comparable to coding algorithms but still providing secrecy against attacks from resource-bounded adversaries.

Whenever a message must be shared, the middleware has to decide which paths to use, in how many parts divide a message and how many shares will be necessary to recover the whole message. Path choice involves quality and reliability information, but can also take into account the software platform of each device or the technology of each network in the paths between the message source and its destination. Those parameters allow computation of paths that resist to attacks in different software platforms or network technologies [4]. Since security vulnerabilities are usually platform-dependent, this strategy can assure that the communication remains private even in face of malicious attacks against vulnerable platforms.

4 Implementation Challenges in the Context of PLASTIC

Implementation of message redundancy and message sharing in hybrid mobile ad hoc networks presents many practical challenges. There are issues related to the physical wireless layer, for instance how to avoid interferences when simultaneously using multiple wireless interfaces or to the architecture such as the integration of multi-path routing with service discovery to rank results according to multi-path availability. In this section, however, we discuss the challenges related to the implementation of multi-path routing as a middleware-provided communication primitive.

Routing Protocol Each network integrated in a HMANET is autonomously organized and runs the routing protocol better adapted to its local requirements. As such, it is unfeasible to define a single routing protocol to be executed by all devices on a HMANET, including bridges. Rather, a more suitable solution to

allow for packet routing among networks is to create an overlay network containing bridges that run a bridge-to-bridge routing protocol while local delivery on each network is performed using the network-specific protocol. To explore multi-path routing on the overlay network, thus, each bridge must learn from the routing protocol all available paths to a destination. Traditional MANET routing protocols, however, keep only a single path between nodes, more specifically the path with the smallest number of hops [17, 6, 5]. Multi-path extensions to those protocols exist, but some of them only use a secondary route if the main route breaks [10, 13] or only compute network-disjoint routes [15], while our scenario requires discovery of network-disjoint, bridge-disjoint and totally-disjoint routes.

The routing protocol must also provide additional information about each network and each node such as available bandwidth, technology, security properties, trust and delay. Additionally, bridges must be able to define the whole path used by each packet to reach its destination. This is necessary to ensure that the packets will follow different routes. Protocols based on routing tables, hence, are not appropriate since each node keeps a local routing table and autonomously forwards packets to the next hop towards the packet destination; different packets to the same destination will always be forwarded to the same next hop. A more adequate technique to forward packets is source route [6], where the source node includes in the packet header the whole path that the packet must follow to reach the destination. As such, the source can define in the packet headers that two packets addressed to the same destination must traverse disjoint paths.

We designed a hybrid ad hoc routing protocol that uses source routes to forward packets and thus ensures that the path defined at the packet source will be respected during packet transmission. The protocol also proactively keeps the shortest route to every node on the network using the efficient flooding mechanism proposed by OLSR [5] while multiple paths to a destination are discovered on demand by using a technique similar to DSR [6]. Route announcements contain not only connectivity information but also quality information such as network throughput, delay, software platform and cost. This protocol provides single-path routing without extra cost and reduces the overhead of multiple route discovery only to situations where a node requires multi-path routing.

Multi-path Granularity There are two issues related to granularity in multi-path applications. The first issue, which is more often discussed in the literature, is traffic allocation granularity [8, 9], which defines the smallest traffic unit that can be assigned to each path. From the application standpoint, the smallest unit is a message. However, in the network layer, a message can originate a number of packets depending on its size and on the network's maximum transmission unit (MTU). Per message allocation enables different messages to follow different routes while in per packet allocation different packets from the same message can use different paths.

Implementing per message traffic allocation when devices feature multiple network interfaces is not straightforward. Messages from the same connection

can arrive through different interfaces from distinct source IP addresses, but the Internet Protocol suite cannot keep a session across different source and destination addresses. In that case, the middleware must implement some type of session management mechanism, on top of the IP stack, to identify related messages and to deliver relevant messages to applications. Per packet allocation is trickier to implement, since different packets from the same message may arrive through different addresses to the destination. For TCP connections, this would require modifications on the IP stack. However, we can use UDP messages to encapsulate each packet and then use the same middleware layer on top of IP to reconstruct application messages.

The second issue is path selection granularity. Paths can be defined per connection, per message or per packet. Considering that nodes in hybrid mobile ad hoc networks are mobile, paths may change frequently. Routes found at the beginning of a connection may not be available towards its end depending on how often nodes move or how long the connection lasts. However, smaller granularities can cause unnecessary overhead. The best strategy, hence, is to select a set of paths when creating a connection, and reselect them after a pre-defined period of time or when a certain number of paths are disconnected.

Network Density Availability of multiple paths between two nodes is highly dependent on bridge deployment. Bridges connect different networks and can increase network density if conveniently deployed. Current PLASTIC strategies for bridge election only take into account resource availability. This strategy can be improved to incorporate the current network topology, for instance, to prioritize bridges that increase network density regardless of the resources they provide. The election algorithm can also consider properties such as stability and trust on networks and bridges to elect new bridges that provide alternative paths to untrusted or unreliable nodes.

Finally, bridges can be temporarily enabled to create a short-lived alternative route to a required destination. Whenever a node not acting as a bridge receives a route request for an alternative route, it may forward the route request to neighbor networks and became a bridge if it discovers an alternative route. An incentive mechanism could be used to stimulate nodes to share resources and act as bridges.

5 Conclusion

Multi-path communication can provide greater reliability and improve privacy of message transmissions. By simultaneously using multiple paths to send the same message, or parts of one message, applications can increase the probability that a message will reach its destination and make it harder for an attacker to read its contents. Those properties are particularly important in mobile and infrastructure-less networks with unstable topologies where untrusted user devices forward packets.

We propose the introduction of an additional layer to the PLASTIC middleware, responsible for handling multi-path communication issues. Figure 3 shows

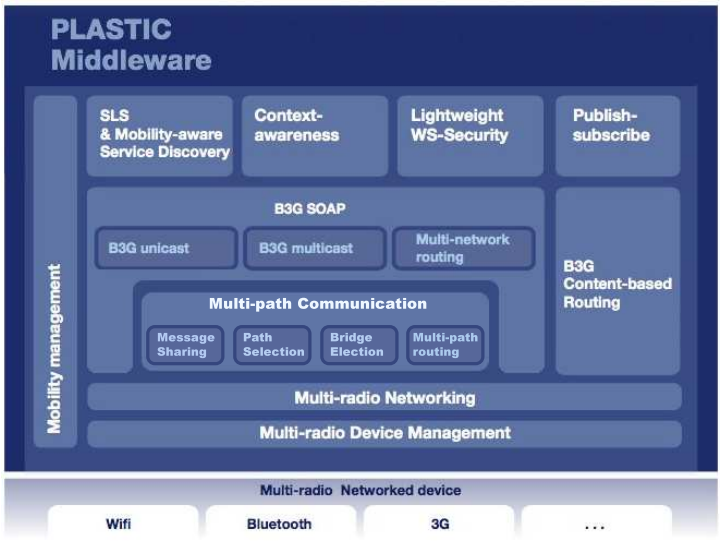

Fig. 3. Multi-path Communication Layer on PLASTIC Middleware

the position of the Multi-path Communication layer in the PLASTIC Middleware architecture. This layer uses functionalities provided by the Multi-radio Networking layer such as the ability to send packets through different interfaces or to resolve a PLASTIC Address into its corresponding set of valid IP addresses. The Multi-path Communication layer, however, is optional: whenever a SOAP message must be sent through a single path, the B3G SOAP layer can dispatch it directly to the Multi-radio Networking layer.

The multi-path routing component uses a hybrid routing protocol (proactive and reactive) to reduce routing overhead; multi-path routing messages are only transmitted when multi-path communication is necessary. The Message Sharing and the Path Selection components rely on information obtained by the Multi-path Routing component, and are also only used when the application requires stronger reliability or privacy.

We are now developing the Multi-path Communication layer. We plan to evaluate the processing and network overhead produced when simultaneously using different paths to transmit a message and we are now evaluating the energy cost imposed by the multi-path routing protocol described in Sect. 4 when compared to traditional ad hoc routing protocols. Finally, we also intend to analyze the availability of multiple disjoint paths in HMANETs and to quantify the reliability and privacy benefits provided by the multi-path approach.

Acknowledgment This work is part of the IST PLASTIC project and has been funded by the European Commission, FP6 contract number 026955.

References

1. I. F. Akyildiz, X. Wang, and W. Wang. Wireless Mesh Networks: A Survey. *Computer Networks and ISDN Systems*, 47(4), 2005.
2. E. Ayanoglu, I. Chih-Lin, R. D. Gitlin, and J. E. Mazo. Diversity Coding for Transparent Self-Healing and Fault-Tolerant Communication Networks. *IEEE Transactions on Communications*, 41(11), 1993.
3. L. Csirmaz. The Size of a Share Must Be Large. *Journal of Cryptology*, 10(4), 1997.
4. Y. Desmedt, Y. Wang, and M. Burmester. Revisiting Colored Networks and Privacy Preserving Censorship. In *CRITIS 2006: First International Workshop on Critical Information Infrastructures Security*, 2006.
5. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot. Optimized Link State Routing Protocol for Ad Hoc Networks. In *INMIC 2001: Proceedings of the IEEE International Multi Topic Conference*, 2001.
6. D. B. Johnson, D. A. Maltz, and J. Broch. *Ad hoc networking*, chapter DSR: the Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks, pages 139–172. Addison-Wesley Longman Publishing Co., Inc., 2001.
7. H. Krawczyk. Secret Sharing Made Short. In *CRYPTO '93: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, 1994.
8. R. Krishnan and J. A. Silvester. Choice of Allocation Granularity in Multipath Source Routing Schemes. In *INFOCOM '93: Proceedings of the Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies*, 1993.
9. W. S. Lai. Bifurcated Routing in Computer Networks. *SIGCOMM Computer Communication Review*, 15(3), 1985.
10. S.-J. Lee and M. Gerla. AODV-BR: Backup Routing in Ad Hoc Networks. In *WCNC'00: Wireless Communications and Networking Conference*, 2000.
11. W.-H. Liao, S.-L. Wang, J.-P. Sheu, and Y.-C. Tseng. A Multi-Path QoS Routing Protocol in a Wireless Mobile Ad Hoc Network. *Telecommunication Systems*, 19(3-4), 2002.
12. W. Lou, W. Liu, and Y. Fang. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks. In *INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, 2004.
13. M. K. Marina and S. R. Das. On-demand Multipath Distance Vector Routing in Ad Hoc Networks. In *Ninth International Conference on Network Protocols*, 2001.
14. S. Mueller, R. P. Tsang, and D. Ghosal. *Performance Tools and Applications to Networked Systems*, chapter Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges. Springer Berlin Heidelberg, 2004.
15. A. Nasipuri and S. R. Das. On-demand Multipath Routing for Mobile Ad Hoc Networks. In *International Conference on Computer Communications and Networks*, 1999.
16. M. R. Pearlman, Z. J. Haas, P. Sholander, and S. S. Tabrizi. On the Impact of Alternate Path Routing for Load Balancing in Mobile Ad Hoc Networks. In *MobiHoc '00: Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*, 2000.
17. C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *WMCSA '99: Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications*, 1999.
18. A. Shamir. How to Share a Secret. *Communications of the ACM*, 22(11), 1979.