Study of Seamless Wireless Mesh Network

RAKESH KUMAR

Department of Physics, S. N. S. College, Hazipur, B. R. A. Bihar University, Muzaffarpur, Bihar, India.

ABSTRACT - One of the first commercial mesh networks was Metricoms Ricochet network in the mid- 90s. Ricochet nodes automatically routed client traffic through half-duplex wireless hops until reaching a hard line connection. When the 802.11 standard was ratified in the late-90s, other mesh networks started to emerged. One of these is the MIT Roofnet[1-7] project where tens of access points with roof mounted antennas formed a mesh around campus. Roofnet's emphasis is more on route maintainability and optimization than on handing off a client's connection. Microsoft Research has also done notable work in the area of mesh networks. Their Mesh Connectivity Layer (MCL) creates a wireless mesh network between Windows clients. Their approach focuses on efficient routing protocols and the unique support for multiple radios on each node. Adya, Bahl, Wolman, and Zhou have shown[8] that using multiple radios on a mesh node combined with smart routing algorithms will dramatically improve the throughput of a wireless mesh network. Their work necessitates a specific network driver on all mesh network participants, including the clients. In this present paper our approach requires no such modification to clients, and works across a variety of operating systems.

Keywords – Mesh Network, MCL.

I. Introduction

The IEEE 802.11sMesh Networking standard, analyzed by Camp and Knightly in[36] , specifies three different types of mesh nodes. Mesh points (MP) includes all mesh nodes that participate in the wireless backbone to increase the mesh connectivity. Some mesh points serve as mesh access points (MAP), providing connectivity to clients within their wireless coverage area. Also, some mesh nodes may serve as mesh portals (MPP), connecting the wireless mesh to an external network such as the Internet. In our approach, we assume that every node is potentially an access point, as it increases the availability of the system. Furthermore, other than Internet connectivity, we make no distinction between the capabilities available in nodes that are simply MAP, MPP, or both.

II. Intra-domain Handoff

Cell networks achieve smooth handoff by sharing information between towers about a given mobile device. This session data is used for routing and is updated whenever a phone switches cells[9],[10] . The 802.11 standard lacks the handoff mechanisms available in today's cell network protocols. Mishra, Shin, and Arbaugh analyzed the link-level handoff performance in current 802.11 hardware. Approximately 90%of a handoff delay is attributable to the client adapter scanning for its next AP. Their experiments also illustrate that the practical handoff delay can vary widely depending on the vendors used for the client network card and the AP. Vatn investigated the latency effects of a wireless handoff on voice traffic. His conclusions echo those of Shin and Arbaugh in that the handoff latency can vary widely depending on the hardware vendor used. Since our approach does not require reassociation during handoff, we do not suffer from these vendor specific delays. Ramani and Savage recently demonstrated that a quick link-level handoff is possible on 802.11 networks when the client monitors the signal quality of access points and uses a fast scanning mechanism to listen to all APs in range to choose the best one. Their Sync Scan system has achieved an impressive handoff as low as 5 ms. The fast scanning is achieved through driver modifications to a client's network adapter. In the contrary, our approach uses any unmodified 802.11 client. Two well known general approaches to intra-domain handoff are Cellular IP and Hawaii[11] . A comparison is presented in. In Hawaii, or Handoff-Aware Wireless Access Internet Infrastructure, messages are exchanged between the old gateway and the new gateway for forwarding packets. Cellular IP establishes routes based on traffic from the client, and handoff takes place when a cross-over router is reached. However, applications like Push-to-Talk[12] may require packets to be sent to mobile clients that are only receiving traffic. In addition, these approaches rely on clients initiating the handoff process, and do not address the link level handoff delay present in 802.11 networks when clients reassociates with another access point. Other approaches to intra-domain handoff, such as TMIP and , improve handoff latency in 802.11 networks but do not overcome these limitations. Other general approaches such

DOI : 10.35291/2454-9150.2025.0120

as IDMP , SMIP , and HMIP focus on hierarchy to reduce the global signaling load to improve scalability. In contrast, we provide a complete link-level and network-level solution and propose a novel approach for controlling the handoff from the infrastructure. In[13] , Caceres and Padmanabhan propose the use of gratuitous ARP messages to achieve transparency in the wired infrastructure during handoffs. In their approach, mobile clients initiate the handoff themselves, and the access points send gratuitous ARPs to their upstream routers to create the illusion that mobile clients are always connected to the wired network. The approach requires all access points to be directly connected to the same wired ethernet network.

III. Inter-domain Handoff

Two general approaches for supporting inter-domain handoff are Mobile IP (MIP) and Mobile NAT. In MIP, a client binds to an IP address at the Home Agent (HA). As the mobile client moves to a different access point or domain, it receives a Care-of-Address (CoA) from a Foreign Agent (FA). The mobile client then registers its new CoA with its HA, and data is then tunneled through the HA. Our approach does not require binding the mobile client to a specific Home Agent, but rather ties each connection to the Internet gateway that is closest at the time the connection is initiated. In Mobile NAT, a client receives two IP addresses through DHCP: a binding address for the network stack, and a routing address that will be visible in the network . As the mobile client moves to a different domain, the client may receive a new routing address. However, as end-to-end connections were initiated from the IP address of the network stack, which remains the same, existing connections will be maintained. The approach requires modifying the mobile client network stack to be aware of the protocol, and also changes in the standard DHCP protocol. Our approach does not require any modifications to the mobile client or the DHCP standard. Many reactive approaches have been proposed to address Internet connectivity in wireless ad-hoc networks[14-18] . Some of them provide good connectivity while paying the cost of a fairly high overhead due to periodically advertisements from Foreign Agents, while others adjust slower, using a reactive approach and broadcast advertisements to find Foreign Agents on demand. A hybrid approach that achieves the same connectivity as in pro-active protocols but with less overhead was proposed in. These schemes usually share similarities with Mobile-IP and although they are suitable for ad-hoc networks, they do not perform well in wireless mesh networks. Backbone nodes in a mesh network are stationary, as opposed to the nodes in ad-hoc networks, leaving space to more efficient protocols that exploit the relative stability of the mesh nodes.

Our work also relates to hybrid networks that connect some of the nodes through the wired network to improve efficiency in the use of the wireless spectrum. An interesting problem addressed in deals with interconnecting wireless LANs with cellular networks. This problem is complementary to our work, which focuses on interconnecting wired and wireless networks.

The SMesh Architecture

We consider a set of stationary 802.11 access points connected in a mesh network, and a set of wireless mobile clients that can move within the area covered by the access points. We call each access point a *node* in the wireless mesh network. The mesh topology changes when wireless connectivity between the mesh access points changes, when nodes crash or recover, or when additional nodes are added to expand the wireless coverage. Mobile clients are not part of the mesh topology. Some of the mesh nodes, but not all, have a wired Internet connection. We refer to them as *Internet gateways*. Each mesh node should be capable of reaching its closest *Internet gateway* or any other node via a sequence of hops. The mobile clients are unmodified, regular 802.11 devices that communicate with the mesh nodes to get access to the network. We do not assume any specific drivers, hardware, or software present on the clients. Therefore, *any* regular unmodified mobile device should be able to use the mesh network transparently.

Our goal is to allowmobile clients to freely roam within the area covered by the wireless mesh nodes, with no interruption in their Internet connectivity. All connections (reliable or best effort) opened at mobile clients should not be affected as the clients move throughout the coverage area served by the wireless mesh. Following the above goals, we implemented SMesh [16,17], a system that is capable of providing seamless wireless connectivity to mobile clients. The software architecture of SMesh is shown in Figure 1. Below we describe the two main components of the SMesh architecture: the communication infrastructure and the interface with mobile clients.

DOI : 10.35291/2454-9150.2025.0120

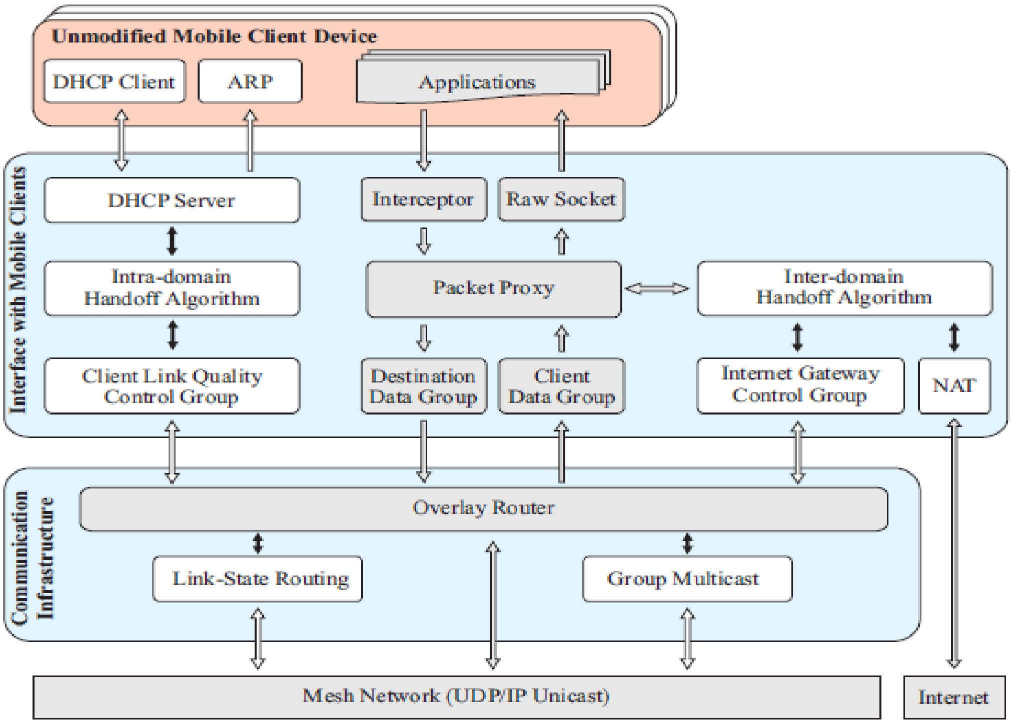

Unmodified Mobile Client Device
DHCP Client
ARP
Applications
Interface with Mobile Clients
DHCP Server
Interceptor
Raw Socket
Intra-domain Handoff Algorithm
Packet Proxy
Inter-domain Handoff Algorithm
Client Link Quality Control Group
Destination Data Group
Client Data Group
Internet Gateway Control Group
NAT
Communication Infrastructure
Overlay Router
Link-State Routing
Group Multicast
Mesh Network (UDP/IP Unicast)
Internet

Fig 1 : The SMesh Architecture

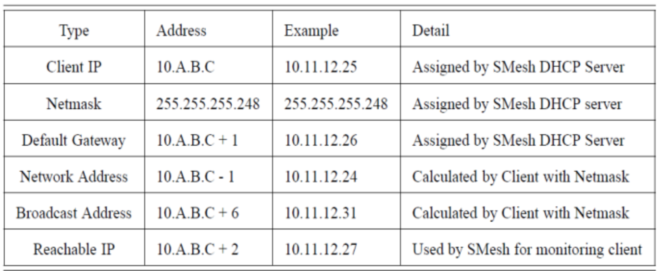
IV. Interface with Mobile Clients

SMesh provides the illusion of a single distributed access point to mobile clients. This is achieved by providing connectivity information to clients through DHCP, and by routing client packet through the overlay network.

Mobile Client Connectivity: The DHCP Server running at each mesh node (access point) is in charge of providing network bootstrap information, including a unique IP address, to a requesting client. We compute this IP address using a hash function on the client's MAC address, mapped to a class A private address of the form 10.A.B.C. A small portion of the private IP addresses in this range is reserved for SMesh nodes, and the rest are available to mobile clients. In case of a hash collision, the client with the smallest MAC keeps the current IP and any other client in the collision gets a managed IP. This scheme decreases the amount of IP management in the network, while assuring that each client gets the same IP address from any SMesh node.

Of particular importance in the DHCP protocol are the *Server ID*, *Default Gateway*, and the T1, T2 and *Lease* timers. The *Default Gateway* specifies the next hop router to use at the MAC level when sending to an IP address outside the client's net mask. The *Server ID* specifies the DHCP Server IP address that the client should contact to renew its lease. The T1 and T2 timers specify when to start unicasting or broadcasting DHCP requests (DHCPREQUEST), and the *Lease* timer specifies when the client must release the IP address. After the *Lease* timer expires, all the connections at the client are terminated. If the access point responds to a DHCP request before the client's Lease time expires, it is able to keep all connections open. In SMesh, the lease time is set to 90 seconds, which gives a client enough time to reconnect in case it goes out of range of any of the mesh nodes temporarily.

Table 1. shows our addressing scheme. We set the netmask of the client to a very small network, thus forcing the client to send packets destined to the Internet or a peer through its default gateway. The default gateway is a virtual IP address; there is no node in SMesh with that IP address. Instead, SMesh makes the client "believe" that this address is reachable by associating this IP address to a mesh node hardware address. This forces the client to route packet through SMesh.



Type	Address	Example	Detail
Client IP	10.A.B.C	10.11.12.25	Assigned by SMesh DHCP Server
Netmask	255.255.255.248	255.255.255.248	Assigned by SMesh DHCP server
Default Gateway	10.A.B.C + 1	10.11.12.26	Assigned by SMesh DHCP Server
Network Address	10.A.B.C - 1	10.11.12.24	Calculated by Client with Netmask
Broadcast Address	10.A.B.C + 6	10.11.12.31	Calculated by Client with Netmask
Reachable IP	10.A.B.C + 2	10.11.12.27	Used by SMesh for monitoring client

Table 1. SMesh IP address assignment scheme

While each client in SMesh consumes 3 bits from the address space, there are still 21 bits available, which allows us to support over one million client IP addresses.

Packet Proxy: Mesh nodes serve as default gateways for the mobile clients. A Packet Proxy module, depicted in Figure 3.1, uses an interceptor to grab packets from a client, and a raw socket interface to forward packets back to the client. Each mobile client is associated with a unique

DOI : 10.35291/2454-9150.2025.0120

multicast group to receive data (Client Data Group). One or more mesh nodes that are in the vicinity of a client will join that client's Data Group. All the Internet gateway nodes are members of a single anycast group.

If the destination of a packet is a SMesh client, the packet is sent to the SMesh nodes that joined that client's Data Group. The mesh node sending this packet can be the Internet Gateway (for packets coming from the Internet) or a sending client access point (for packets originated by a different SMesh client). Upon receiving a packet for the client, each of the SMesh nodes that joined that client's Data Group forwards the packet to the client. If the destination of a packet is the Internet, then the packet is sent by the originating client's access point to the closest Internet gateway by forwarding it to the anycast group. The Internet Gateway will then forward the original packet to the Internet using Network Address Translation (NAT). When a response packet is received from the Internet, a reverse NAT is performed and the packet is sent to the appropriate Client Data Group.

Spines forwards the packets to the members of the client's Data Group using a multicast tree. This way, if the mobile client moved, and a different SMesh node joins the client's Data Group, the packets are forwarded to the newly joined SMesh node. The SMesh node(s) in the Client Data Group use a raw socket to deliver the packet, allowing the mobile client to receive the packets unmodified as if it had a direct connection to the end host. If there are multiple nodes in the Client Data Group, the client could receive duplicate IP packets. However, duplicate IP packets are dropped gracefully at the receiver (TCP duplicates are dropped at the transport level, and applications using UDP are supposed to handle duplicates).

Transparent Overlay Proxy: Application level overlay networks forward packets through application level routers, thus requiring packets to traverse user space. RON used this approach with a special divert socket to increase resilience in the Internet. SMesh intercepts clients packets and sends them through the Spines overlay network to the access points serving the destination. The overlay may span wireless and wired links, and routes may take advantage of the wired network to optimize wireless usage. Once the packets are received by the destination's access points, SMesh strips the overlay headers and forwards the original packet to the mobile client using a raw socket. Unlike RON, our interceptor relies only on a packet sniffer socket, which is readily available in most operating systems, as well as filter and firewall settings, to perform this task.

Conclusions

In our approach, we use the libpcap library, a well known application level interface for user-level packet capturing. In addition, to improve performance, we use Berkeley Packet Filters [19] to ignore unwanted packets in the kernel. The mesh nodes configure each node as follows:

- • Disable packet forwarding so that the overlay is the only one forwarding packets in the mesh network.
- • Drop any packet destined to the Internet IP address of mesh nodes connected to the Internet.
- • Filter out every port used by the overlay network to ensure that these packets are not captured.

Spines uses four different ports to communicate between daemons. When a mesh node receives a packet destined to an IP address that is not its own (i.e., when a mobile client sends a packet destined to the IP address of Goggle), the kernel attempts to route the packet, and when unsuccessful it drops the packet to the floor. However, the packet sniffer socket gets a copy of the packet, which SMesh then send through the Spines overlay network to its appropriate destination.

REFERENCES

[1]. “Ieee standard for local and metropolitan area networks part 16: Air interface for fixed broadband wireless access systems,” IEEE 802.16- 2004, 2004.

[2]. R. Draves, J. Padhye, and B. Zill, “Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks,” in Proc. of ACM MOBICOM, Philadelphia, Pennsylvania, USA, 2004.

[3]. Yair Amir, Claudiu Danilov, Michael Hilsdale, Raluca Musaloiu-Elefteri, and Nilo Rivera. Fast handoff for seamless wireless mesh networks. In MobiSys 2006, pages 83–95, New York, NY, USA, 2006. ACM Press.

[4]. H. Schulzrinne and S. Petrack. RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals. RFC 2833, May 2000.

[5]. Roger M. Whitaker and Steve Hurley. Evolution of planning for wireless communication systems. In IEEE Hawaii International Conference on System Sciences (HICSS), 2003.

[6]. D. Tang and M. Baker, “Analysis of a Metropolitan-Area Wireless Network,” ACM/Kluwer Wireless Networks. Special issue: Selected Papers from Mobicom’99, vol. 8, no. 2/3, pp. 107–120, 2002.

[7]. B. A. Chambers, “The grid roofnet: a rooftop ad hoc wireless network,” Master’s thesis, Massachusetts Institue of Technology, May 2002. [Online]. Available: citeseer.ist.psu.edu/chambers02grid.html

[8] A. Adya, P. Bahl, J. Padhye, A.Wolman, and L. Zhou, “A multi-radio unification protocol for IEEE 802.11 wireless networks,” in *BROADNETS ’04: Proceedings of the First International Conference on Broadband Networks (BROADNETS’04)*. Washington, DC, USA: IEEE Computer Society, 2004, pp. 344–354.

DOI : 10.35291/2454-9150.2025.0120

[9] Y. Bejerano, I. Cidon, and J. S. Naor, “Efficient handoff rerouting algorithms: a competitive on-line algorithmic approach,” *IEEE/ACM Trans. Netw.*, vol. 10, no. 6, pp. 749–760, 2002.

[10] C.-F. Chiasserini, “Handovers in Wireless ATM Networks: In-Band Signaling Protocols and Performance Analysis,” *IEEE Transactions on Wireless Communications*, vol. 1, no. 1, Jan 2002.

[11] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, and S. Wang, “Hawaii: a domainbased approach for supporting mobility in wide-area wireless networks,” *Network Protocols, 1999. (ICNP ’99) Proceedings. Seventh International Conference on*, pp. 283–292, Oct.-3 Nov. 1999.

[12] L. DaSilva, G. Morgan, C. Bostian, D. Sweeney, S. Midkiff, J. Reed, C. Thompson, W. Newhall, and B. Woerner, “The resurgence of push-to-talk technologies,” *Communications Magazine, IEEE*, vol. 44, no. 1, pp. 48–55, Jan. 2006.

[13] R. Caceres and V. N. Padmanabhan, “Fast and Scalable Wireless Handoffs in Support of Mobile Internet Audio,” *ACM Journal on Mobile Networks and Applications*, vol. 3, no. 4, pp. 351–363, 1998.

[14] A. A.-G. Helmy, M. Jaseemuddin, and G. Bhaskara, “Multicast-based mobility: A novel architecture for efficient micromobility,” *IEEE Journal on Selected Areas in Communications*, 2004.

[15] A. Forte and H. Schulzrinne, “Cooperation between stations in wireless networks,” *Network Protocols, 2007. ICNP 2007. IEEE International Conference on*, pp. 31–40, Oct. 2007.

[16] Y. Amir, C. Danilov, M. Hilsdale, R. Musaloiu-Elefteri, and N. Rivera, “Fast handoff for seamless wireless mesh networks,” in *MobiSys 2006: Proceedings of the 4th international conference on Mobile systems, applications and services*. New York, NY, USA: ACM Press, 2006, pp. 83–95.

[17] Y. Amir, C. Danilov, R. Musaloiu-Elefteri, and N. Rivera, “An inter-domain routing protocol for multi-homed wireless mesh networks,” *International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2007), Helsinki, Finland*, June 2007.

[18] W. Matthew, J. Miller, and N. Vaidya, “A hybrid network implementation to extend infrastructure reach,” *UIUC Technical Report*, 2003. [Online]. Available: citeseer.ist.psu.edu/matthew03hybrid.html

[19] S. McCanne and V. Jacobson, “The bsd packet filter: a new architecture for user-level packet capture,” in *USENIX’93: Proceedings of the USENIX Winter 1993 Conference Proceedings on USENIX Winter 1993 Conference Proceedings*. Berkeley, CA, USA: USENIX Association, 1993, pp. 2–2.

DOI : 10.35291/2454-9150.2025.0120