

Evaluation of Wireless Mesh Network Handoff Approaches for Public Safety and Disaster Recovery Networks

Ryan Wishart*, Marius Portmann*[†], Jadwiga Indulska*[†]

Queensland Research Laboratory*

NICTA

Brisbane, Australia

The University of Queensland[†]

School of Information Technology and Electrical Engineering

Brisbane, Australia

{ryan.wishart, marius.portmann, jadwiga.indulska}@nicta.com.au

Abstract—In Public Safety and Disaster Recovery (PSDR) scenarios, reliable communication is an imperative. Unfortunately, communication infrastructure is often destroyed or overwhelmed by whatever precipitated the scenario (e.g., a hurricane or terrorist attack). Thus, the PSDR workers must often deploy their own communications infrastructure on-site. Wireless mesh networks (WMN) have been identified as being ideally suited to this task. WMN offer a high-capacity wireless backhaul network, provided by mesh routers, through which clients can connect to one another or with external networks. Mobility of clients within the mesh is particularly important for Public Service and Disaster Recovery scenarios. This creates a challenging problem as clients may move out of range of the mesh router they were using to connect to the mesh and need to associate with another. Client handoff mechanisms provide this functionality. In this paper we provide a critical survey of client handoff approaches applicable to IEEE 802.11 WMN evaluating them based on the strict QoS requirements established by the US Department of Homeland Security for PSDR networks.

Index Terms—client handoff, mesh networks, mobility, wireless networking, Public Safety and Disaster Recovery, Incident Area Networks

I. INTRODUCTION

Temporary communications infrastructure is often required by the Public Safety and Disaster Recovery (PSDR) workers when they arrive at the scene of a disaster. Wireless mesh networks are ideal for establishing this temporary communications infrastructure [1] as they provide broadband connectivity over a wide area and can be rapidly deployed (due to their self-configuring and self-healing functionality). In wireless mesh networks there are typically two categories of node present: mesh clients and mesh routers [2].

Mesh clients are wireless-enabled, portable devices such as PDAs. These devices typically have limited power and computational resources.

Mesh routers function as dedicated router devices that connect to one another to form the wireless, multi-hop backbone of the mesh network. While it is possible that mesh routers

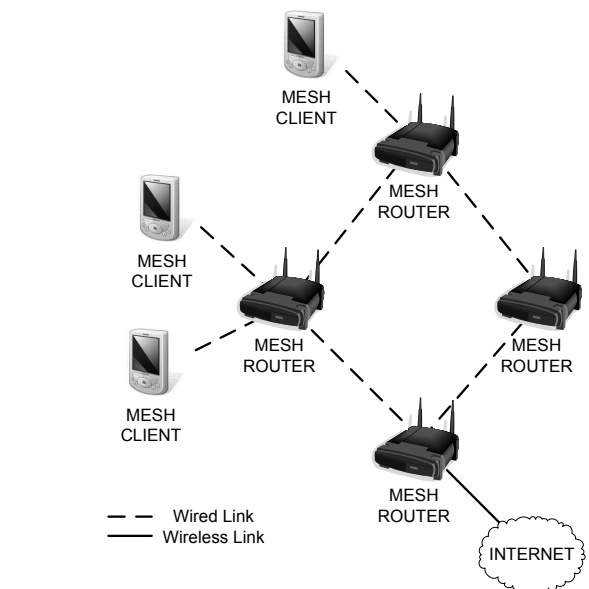


Fig. 1. An Infrastructure Mesh Network

are mobile, they are typically treated as static nodes within the mesh network. Mesh routers usually have significant power resources (such as a connection to mains power) and, quite often, more than one wireless interface.

Within the context of this paper we focus on infrastructure mesh networks, one of the three classes of mesh network identified by Akyildiz *et al.* in [2]. The other classes being *client mesh networks*, similar to ad hoc networks [3], and *hybrid mesh networks* (where clients are able to perform routing). An example infrastructure mesh network is shown in Figure 1.

Within this paper we will use the term *client device* to describe a mesh client that does not engage in routing or forwarding of another node's traffic. These client devices must send all their traffic to a special mesh router, termed an *access router*, in order to use the mesh backhaul network. This access

router must be one hop away.

In Public Safety and Disaster Recovery networks the client device role is filled by Public Safety Communication Devices (referred to as PSCDs) [4] that are carried by the PSDR workers. As these workers may be using vehicles on an incident site, the PSCDs they carry can exhibit very high mobility [5]. To prevent communication dropouts when a PSCD moves out of range of its current access router, a mechanism is needed to locate and arrange a graceful handoff to a new access router. So as not to breach the strict QoS requirements established in [4] for PSDR networks, the handoff must occur quickly with no packet loss and minimal overhead.

In this paper we evaluate existing handoff approaches that operate at layer-2 and layer-3 of the network stack. This evaluation is done using a set of requirements drawn from the SAFECOM Public Safety Statement of Requirements Reports issued by the United States Department of Homeland Security [5][4].

The remainder of this paper is structured as follows. In Section II we provide background information regarding handoffs in 802.11 networks. In Section III we then outline the basic structure of Public Safety and Disaster Recovery networks and present the handoff performance requirements. A critical literature survey is performed in Section IV followed by a discussion in Section V. The paper is concluded in Section VI.

II. BACKGROUND

In order for a client device to change its access router, a handoff must occur at layer-2 of the network stack. A layer-3 hand-off may also be required if the new access router is in a different subnet. Layer-3 handoffs are quite specific to the protocol used, whereas layer-2 handoffs all modify the default handoff behavior described in IEEE 802.11 a/b/g (the predominant networking standards used by existing wireless mesh networks). As such, we only cover layer-2 handoffs in this section.

The complexity of the layer-2 handoff is highly dependent on the network mode which the client device uses to connect to the access router. In IEEE 802.11 a/b/g, two modes are possible: *infrastructure* and *ad hoc*.

A. Infrastructure mode

In the terminology used with infrastructure mode, a client device is referred to as a “station”, while the access router is termed an “access point”.

In standard infrastructure mode, the station controls the handoff procedure and is responsible for:

- Determining that a handoff is necessary
- De-associating with the current access point
- Scanning the 802.11 channels looking for another access point
- Authenticating to the new access point
- Re-associating with the new access point

Of these steps, the most time consuming is scanning for another access point to handoff to. During this scanning process the station must listen on all of the 802.11 channels

for beacon frames sent by access points. These beacon frames contain information on the channel used by the access point, the network identifier for the wireless network, information pertaining to power management, supported transmission rates, etc.

In the best case, scanning can be completed in 350ms to 500ms [6] (depending on the station/access point hardware). In the worst case it can take longer than a second [7].

Importantly, while scanning for access points the station is unable to send or receive data frames.

B. Ad hoc mode

In IEEE 802.11 ad hoc mode, nodes connect directly to one another in a peer-to-peer manner meaning there are no access points. As there is no formal relationship between the client device and the access router, handoffs are less complicated than in infrastructure mode. In particular, de-association and re-association are not needed.

It should be noted that in this survey we do not consider authentication time as this is highly dependent on the authentication algorithm used. The default open system authentication can be completed very quickly, requiring only the exchange of two frames. More sophisticated authentication, such as 802.11x, introduces additional delay particularly if a remote server has to be contacted.

III. PSDR NETWORK STRUCTURE AND REQUIREMENTS

In Public Safety and Disaster Response scenarios, an hierarchical network structure is used to ensure scalability.

At the bottom layer of the hierarchy are Personal Area Networks (PAN). These correspond to small wireless networks connecting various sensors and communication devices together on a PSDR worker.

When PSDR workers first arrive at an incident site, they establish an Incident Area Network (IAN) to provide temporary, on-site wireless connectivity between their individual PANs. As time is critical in public safety and disaster scenarios, IANs need to be rapidly deployable, self-healing and self-configuring [5]. In addition they need to support high-quality video, voice and data services, be highly scalable (both in terms of the number of nodes and in coverage area) and also function despite high node mobility. This mobility includes nodes moving between access routers within the IAN, as well as between IANs.

Permanent Jurisdiction Area Networks (JANs), corresponding roughly to cities, provide connectivity between the IANs.

Connectivity between JANs is facilitated by an Extended Area Network (EAN). This network spans inter-city, regional, state and national scales.

Within this paper we focus on client device (e.g., a PSCD) handoffs within Incident Area Networks. We consider the JAN equivalent to a network domain, and the IANs within it as subnets belonging to that domain.

A summary of the relevant network performance requirements, taken from [5] is given below:

- The first is to support PSCD mobility. This necessitates the existence of a handoff mechanism that can handoff active sessions (such as voice calls and video streams) between IANs.
- An additional requirement is that the network should be scalable. In terms of the handoff mechanism, scalability can be increased by minimising the amount of network signaling that occurs for each handoff (such as routing table or gateway updates and redirections through the network).
- The last, and most challenging, of the requirements is that IAN networks used in PSDR applications support the packet loss and latency values given in Table I. Consequently, the handoff procedure cannot induce packet loss and may only create delay in the IAN of less than 14ms. These values were sourced from [4], Section 7.4, pp 73.

IV. EVALUATION OF EXISTING CLIENT HANDOFF APPROACHES

In this section of the paper we use the requirements given in Section III to evaluate handoff approaches operating at layer-2, layer-3 and those that are operate across these layers (i.e. are cross-layer). We do not include the approaches used within commercial mesh networking products as the necessary details are not readily available.

A. Layer-2 Handoff Approaches

1) *SyncScan*: SyncScan, developed by Ramani and Savage [8], is a layer-2 client device handoff approach for IEEE 802.11 infrastructure mode networks.

When using the SyncScan approach, a client (equipped with one wireless NIC) is required to scan the 802.11 channels for beacons from access points at regular intervals. This means that should a client decide a handoff is necessary, it can skip the scanning phase of the handoff process as it already has an up-to-date list of access points and their channels. By removing the scanning phase, SyncScan handoffs can be completed extremely quickly.

To ensure that the client does not have to spend much time waiting for beacon broadcasts, the client's periodic channel scans are synchronized with the access point beacon broadcasts.

While performing the periodic channel scan, the client is unable to receive frames from the access point. Ramani and Savage suggest the client inform the access point that it is entering Power Saving Mode (PSM). This will cause the access point to buffer outgoing frames to the client until the client returns to the channel. Likewise, the client will have to buffer its outgoing frames for the access point until it returns to the channel.

By using the SyncScan approach clients can handoff between access points in as little as 7ms [8]. This is well within the PSDR QoS requirements. That said, the periodic scanning approach may result in a violation of the 14ms cap on latency if the client has to wait longer than 4ms for the access point beacons (each periodic scan requires two channel switches costing 5ms [8] each).

2) *Make-Before-Break*: In the Make-Before-Break approach, presented by Ramachandran et al. [7], two network interfaces are used on the client device. One of these interfaces is used for sending/receiving data while the other is used to scan the 802.11 channels for beacons from access points.

When an access point with significantly better signal quality is located, a handoff is performed by the client. This handoff process involves *first* using the scanning interface to associate with the new access point and *then* breaking the association with the old access point. The two interfaces then swap roles with the scanning interface being used for data transfer, and the previous data transfer interface switching to scanning for access point beacons.

The total handoff latency associated with the approach (that is, the time for the probing interface to associate with the new access point and for the two interfaces to swap roles) is below 10ms.

The approach improves on SyncScan in that it does not suffer from lost frames and does not require synchronized broadcast of beacon messages by the access points. Additionally, the latency involved with the handoff procedure is less than the 14ms permitted network latency in PSDR IAN networks.

A drawback of the approach is that the client must be equipped with two wireless NICs.

3) *802.11r*: The 802.11r [9] standard is designed to enable fast handoffs between access points for highly mobile clients. This is achieved by addressing the delays introduced by Quality of Service (QoS) establishment and authentication during the handoff procedure.

The standard enables a client to request QoS resources either when re-associating with the new access point or prior to the handoff procedure (using its current access point as a conduit).

Authentication is also expedited by the introduction of a new key management system that enables clients to perform security operations prior to the handoff [10].

The approach has been reported to significantly reduce handoff times from more than 500ms to approximately 42ms [10]. This is achieved with minimal packet loss (less than 1%) while also providing EAP 802.11x authentication of the client. It should be noted that QoS reservation was not used in the tests that produced these results.

While 802.11r significantly improves the performance of the standard 802.11 handoff procedure, it fails to meet the delay and packet loss requirements specified for PSDR networks.

B. Layer-3 Handoff Approaches

1) *Mobile IP*: Mobile IPv4 [11] provides layer-3 mobility by providing a single IP address at which a client device can be reached regardless of the network it is located in.

In the approach, the client device's IP address on its home network becomes the identifier for the client.

Whenever the client device attaches to a foreign network, it registers with a Foreign Agent (FA) in that network. The FA is responsible for informing the Home Agent in the client's home network. This process also sets up a tunnel through which traffic for the client that arrives at the home network is forwarded to the new network.

TABLE I
SOFT REAL-TIME LIMITS FOR PSDR VOICE AND VIDEO COMMUNICATIONS THROUGH AN IAN.

Communication Mode	Packet Loss Probability	Maximum Latency
Voice communications	0	14ms
Video Communications	0	14ms

An additional problem with standard Mobile IPv4 is the delay introduced by the FA registration process. Only once registration is complete can traffic be forwarded to the client in its new network. Delay introduced by this registration process can be significant [12]. In PSDR networks highly mobile client devices that move between IANs would experience delay significant enough to disrupt any active voice or video sessions.

As with Mobile IPv4, Mobile IPv6 [13] permits hosts to communicate with a client using a single address, regardless of the actual network to which the client is currently attached. However, unlike Mobile IPv4 (which is distinct from IPv4), Mobile IPv6 is tightly integrated with the IPv6 protocol. This simplifies the process of supporting client device mobility leading to performance improvements.

Some benefits of Mobile IPv6 with respect to PSDR networks include:

- Foreign Agents, required by mobile IP v4 in each network to track the location of client devices, are no longer necessary in Mobile IPv6 as the protocol is able to run in any IPv6 network
- Tunneling between the client device's home network and the visited network is no longer necessary in Mobile IPv6. Rather, an IPv6 routing header is used to indicate the destination address of the packet. This reduces the amount of overhead compared to Mobile IPv4 [13].

2) *NeighborCasting*: In the NeighborCasting approach developed by Shim *et al.* [14], Mobile IPv4 is extended to provide fast handoffs for client devices.

When a client intends to move to another network, it sends the Foreign Agent FA_{old} in its' current network a Handoff Notification. FA_{old} then sends all neighboring FA a Forwarding Notification message, signaling its intent to forward traffic for the client. Any traffic for the client that arrives during the handoff period is then automatically forwarded by FA_{old} to all neighboring FAs.

As soon as the client completes layer-2 association with another network, the FA for that network can forward any queued packets from FA_{old} to the client. Provided the FA_{new} is informed of the client's MAC address in the Forwarding Notification sent by FA_{old} , this can occur even while the Mobile IP registration process is occurring. As such, the delay introduced by the NeighborCasting protocol can be very small (approximately 5.5ms). It should be noted that this value does not include the layer-2 handoff process. The approach also avoids packet loss, though this is at the expense of increased traffic on the backhaul network.

When evaluated using the criteria established in Section III, NeighborCasting satisfies the mobility and QoS requirements. When applied to a wireless mesh network, the need to multicast traffic to multiple FAs during client handoffs

means that the approach may be unable to meet the scalability requirements when dealing with high-bandwidth flows (e.g., high-quality video).

3) *Cellular IP*: Cellular IP is a micro-mobility approach developed by Campbell *et al.* [15] that operates with infrastructure mode wireless networks. In the approach, a mobile client device uses its home network address as its identifier.

All traffic from a client is assumed to be sent via the network gateway. These uplink packets are used to maintain a route to the client. Packets sent to the client use the reverse route. When a client has no data to send it transmits ICMP packets to the gateway to keep its uplink route active.

When the client device detects the need for a handoff to another access point, it can either employ a hard handoff approach, or a semi-soft approach.

In the hard handoff approach the client switches to another access router. On completion of the layer-2 handoff the client transmits a route update packet to the gateway to inform it of the change of location. Routers forwarding the packet note the change in origin and update their routes to the client accordingly.

In the soft-handoff approach, the client quickly switches over to the new access point (assuming both access points are within range) and transmits a soft-handoff packet before changing back to its old access point. This creates a new route for the client in the new subnet. Packets for the client are then sent to the old access point (on which the client device is still listening) and also to the new access point.

To remove the need for the small ICMP packets to maintain a route when the client is not sending data, a paging mechanism can be used. This mechanism divides the domain into different cells. The client only needs to report its location to the gateway when it changes cell. When a packet arrives for the client, the client is paged in its last known cell. The client responds to the page, creating a route that can be used to send the packet.

Cellular IP is not able to meet the PSDR requirements as the hard handoff mechanism results in the loss of packets and introduces delay into the handoff process (with the delay being equal to the layer-2 handoff in addition to the amount of time to create a route to the gateway).

During the semi-soft handoff packet loss can occur while the client switches to the new access router, sends its soft-handoff packet, and then switches back to its old access router. Again, these losses violate the PSDR requirements.

C. Cross-Layer Handoff Approaches

1) *SMesh*: In SMesh, developed by Amir *et al.* [16], mesh routers use one of their wireless interfaces exclusively for communicating with clients. As with LIHP, all mesh routers configure their client interface with the same well-known IP

address. Clients then use this well-known IP address as their default gateway connecting to it using 802.11 ad hoc mode.

In the approach DHCP is used to configure clients. Short DHCP lease times ensure that the client frequently sends IP renewal messages. Mesh routers receiving these messages keep track of the client's location and the quality of their link to the client.

Mesh routers with a high quality link to the client join a multicast group for that client. All the members of the client's multicast group forward traffic to the client. This means that the client may receive duplicate IP packets when there is more than one mesh router in its multicast group. If one mesh router has significantly better link quality than all the others, the multicast group quickly shrinks to just that router.

As a client receives duplicate IP packets from all members of its multicast group, SMesh has the ability to flood a noisy channel with a large number of duplicate packets sent by the multicast group members.

SMesh's dependence on DHCP for configuring and discovering clients also has significant drawbacks. The cost of reconfiguring a device via DHCP is platform-dependant and can induce delay of up to 5 seconds [17].

Handoffs between access routers in SMesh result in lost packets, receipt of duplicate packets and reported handoff times in excess of 100ms. As such, the approach fails to meet the strict requirements of PSDR networks.

2) *LCMIM*: In the Light-Weight Client Mobility Scheme for Infrastructure Mesh Networks (LCMIM), developed by Wishart *et al.* [18], client devices are entirely passive. Handoffs are controlled by the mesh routers who regularly broadcast gratuitous Address Resolution Protocol (gARP) [19] messages from their client interfaces. ARP enables the MAC address associated with an IP address to be discovered on a LAN. This process usually involves an ARP request, followed by a response from the IP address user. Gratuitous ARP messages are typically the response message only.

Client devices in the approach send all their traffic via a special virtual gateway IP address (e.g., 10.0.3.5). All the mesh routers that have a client interface use this virtual gateway IP address on their client interfaces. When the client device receives a gARP from one of the mesh routers, it updates its ARP cache entry for the virtual gateway IP address so that the IP address maps to the MAC address of the sending mesh router.

All outgoing traffic from the client device then travels via the mesh router that most recently sent a gARP message. In a network with high mesh router density, the gARPs may be received from multiple mesh routers. In this case the outbound traffic from the client 'oscillates' between the mesh routers from which the client received gARP messages. As shown in [18], these oscillations have no affect on either TCP or UDP sessions conducted by the client.

In handoff scenarios, the approach offers near instantaneous access router handoff with no packet loss or induced delay. Provided, that is, packets sent by the old access router can still be received post-handoff. For this to occur, the handoff must be between access routers on the same channel.

The potential for packet loss and the need to broadcast

gratuitous ARP messages at regular intervals from all access routers mean that LCMIM is not able to fulfill the packet loss and scalability requirements of PSDR networks.

V. DISCUSSION

Handoffs in the standard infrastructure mode used by 802.11 networks introduces significant delay (ranging between 350ms and 1s) that violates the maximum latency of 14ms that can be introduced for data traversing an IAN. This delay is largely due to the scanning phase of the infrastructure mode handoff.

Client handoff time is significantly reduced in networks supporting the 802.11r standard [9]. A preliminary implementation of the standard by Bangolae *et al.* [10] achieved access point handoff in less than 50ms. Despite these significant improvements, 802.11r is not sufficient to meet the needs of PSDR networks.

Of the layer-2 approaches surveyed only Make-Before-Break [7], which used two wireless interfaces on the client, was able to reduce handoff latency to below 10ms in 802.11 infrastructure mode.

When PSDR client devices move between IANs, a traffic redirection mechanism such as Mobile IP is need. Mobile IPv4 [11] has high registration costs that introduce additional latency into the handoff procedure exceeding what is acceptable within PSDR networks.

For client device movement within a local domain (i.e. a JAN) there are micro-mobility optimization protocols for Mobile IPv4 such as Cellular IP [15]. These approaches reduce the amount of network signaling required (compared to standard Mobile IPv4).

Mobile IPv6 overcomes many of the problems associated with Mobile IPv4 and requires less overhead making it a more suitable alternative to support layer-3 mobility in PSDR networks than Mobile IPv4.

Of the layer-3 approaches surveyed, NeighborCasting [14] offered the fastest layer-3 handoff times (approximately 5ms). This was done by multicasting packets for a client device to the Foreign Agents in neighboring networks. These packets could be received by the client device as soon as it had completed layer-2 handoff. In a mesh network this would only be achievable at the expense of significant additional traffic on the wireless backbone (albeit for short periods of time).

VI. CONCLUSION

The SAFECOM Statement of Requirements reports [5][4], issued by the US Department of Homeland Security, provide a strict set of performance requirements for Public Safety and Disaster Response networks. We evaluated existing client device handoff techniques for wireless mesh networks using a subset of these requirements, namely: (1) handoffs of client devices between IANs should not lead to packet loss, (2) the handoff can only induce less than 14ms latency, and (3) the approach must be scalable.

For PSDR devices moving between access routers within an Incident Area Network, a layer-2 handoff approach is necessary. For those moving between IANs (which we consider equivalent to subnets), a layer-3 handoff mechanism is required in addition to a layer-2 approach.

TABLE II
COMPARISON OF HANDOFF APPROACHES.

Approach Name	Layer	Packet Loss Occurs	Satisfies Latency Requirement	Protocol Overhead
SyncScan	layer-2	No (if using PSM)	Yes	N/A
Make-Before-Break	layer-2	Yes	Yes	N/A
802.11r standard	layer-2	Yes	No	N/A
Mobile IPv4	layer-3	Yes	No	High
Mobile IPv6	layer-3	Yes	No	Medium
Cellular IP	layer-3	Yes	No	Medium
NeighborCasting	layer-3	No	Yes	High
SMesh	cross-layer	Yes	No	High
LCMIM	cross-layer	Yes	Yes	Medium

At layer-3, the NeighborCasting approach [14], offered the fastest layer-3 handoff times (approximately 5ms). This was achieved at the expense of potentially high multicast traffic on the wireless backhaul network.

While not directly considered in our survey, it is worth noting that PSDR networks will likely use client authentication mechanisms aside from the default open system authentication. These mechanisms have the potential to induce significant delay whenever the client changes access router. This delay could be reduced by using the new 802.11r standard potentially in combination with a dual NIC approach like that of Make-Before-Break.

This survey has shown that existing client handoff approaches for wireless mesh networks are not able to satisfy the strict requirements established for PSDR networks.

ACKNOWLEDGMENT

NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Centre of Excellence program; and the Queensland Government.

REFERENCES

- [1] M. Portmann, "Wireless mesh networks for public safety and disaster recovery applications," *Chapter in Wireless Mesh Networking: Architectures, Protocols and Standards*, 2006.
- [2] I. Akylidiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, pp. 445–487, 2005.
- [3] A. Pirzada, M. Portmann, and I. Indulska, "Hybrid Mesh Ad-hoc On-demand Distance Vector Routing Protocol," *Proceedings of the 30th Australasian Computer Science Conference (ACSC2007)*, vol. 29, no. 1, pp. 49–58, 2007.
- [4] *Public Safety Statement of Requirements for Communication & Interoperability*, United States of America, The Department of Homeland Security, August 2006, volume 2, version 1.
- [5] *Public Safety Statement of Requirements for Communication & Interoperability*, United States of America, The Department of Homeland Security, October 2006, volume 1, version 1.2.
- [6] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *ACM Computer Communications Review (CCR)*, vol. 33, no. 2, pp. 93–102, April 2003.
- [7] K. Ramachandran, E. Belding, K. Almeroth, and M. Buddhikot, "Interference-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks," in *Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM'06)*, 2006, pp. 1–12.
- [8] I. Ramani and S. Savage, "SyncScan: Practical Fast Handoff 802.11 Infrastructure Networks," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005)*, vol. 1. IEEE Press, 2005, pp. 675–684.
- [9] IEEE, "IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part II: Wireless LAN Medium Access Control (MAC and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS)," July 2008.
- [10] S. Bangolae, C. Bell, and E. Qi, "Performance Study of Fast BSS Transition using IEEE 802.11r," in *Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC'06)*. ACM, 2006, pp. 737–742.
- [11] C. Perkins, "IP Mobility Support for IPv4," RFC 3220 (Proposed Standard), Jan. 2002, obsoleted by RFC 3344. [Online]. Available: <http://www.ietf.org/rfc/rfc3220.txt>
- [12] A. Campbell and J. Gomez-Castellanos, "IP Micro-Mobility Protocols," *Mobile Computing and Communications Review*, vol. 4, no. 4, pp. 45–53, 2001.
- [13] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support for IPv6," RFC 3775 (Proposed Standard), June 2004. [Online]. Available: <http://www.ietf.org/rfc/rfc3775.txt>
- [14] E. Shim, H. Wei, Y. Chang, and R. Gitlin, "Low Latency Handoff for Wireless IP QoS with Neighborcasting," in *Proceedings of the IEEE International Conference on Communications (ICC 2002)*, vol. 5. IEEE Press, 2002, pp. 3245–3249.
- [15] A. Campbell, J. Gomez, S. Kim, A. Valko, C. Wan, and Z. Turanyi, "Design, Implementation, and Evaluation of Cellular IP," *IEEE Personal Communications*, August 2000.
- [16] Y. Amir, C. Danilov, M. Hilsdale, R. Musaloiu-Elefteri, and N. Rivera, "Fast Handoff for Seamless Wireless Mesh Networks," in *Proceedings of the ACM International Conference on Mobile Systems, Applications and Services (MobiSys 2006)*, 2006, pp. 83–95.
- [17] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, and K. Almeroth, "On the Design and Implementation of Infrastructure Mesh Networks," in *Proceedings of WiMesh 2005*, 2005.
- [18] R. Wishart, A. Pirzada, and M. Portmann, "A Light-Weight Client Mobility Approach for Infrastructure Mesh Networks," in *Proceedings of the 15th IEEE International Conference on Networks (ICON 2007)*. IEEE Press, 2007.
- [19] D. Plummer, "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware," RFC 826 (Standard), Nov. 1982, updated by RFC 5227. [Online]. Available: <http://www.ietf.org/rfc/rfc826.txt>