An Experimental Study of Location Assisted Proactive Handover

A. Dutta, S. Chakravarty[c], K. Taniuchi[b], V. Fajardo[b], Y. Ohba [b], D. Famolari[a], H. Schulzrinne[c]
[a]Telcordia Technologies
[b]Toshiba America Research
[c]Columbia University

Abstract: Traditionally, signal-to-noise ratio of a mobile determines the handoff dynamics of the mobile. But in certain cases, precise location of the mobile augmented by information services, such as IEEE 802.21 MIS, can expedite the handoff with similar performance results. We illustrate an experimental system that takes advantage of the mobile's relative location with the neighboring access point to perform proactive handoff. It keeps track of the current location of the mobile and then uses the information from the neighboring networks to help perform the proactive handoff. Proactive handover technique helps the mobile to communicate with these networks before the handover is complete thereby reducing the delay and packet loss. In some cases, location-assisted handover could prove to be more useful compared to the handover technique based on signal-noise-ratio.

I. Introduction

In a highly mobile environment, where a mobile node (MN), frequently switches network and link associations, it is desirable that existing applications continue to run oblivious of such handoffs. Handoff decision can be policy-based and can be dependent on many factors. Most common ones include the perceived signal-to-noise ratio (SNR), available bandwidth and the type of application being supported in a specific network. Mobility mechanisms help a mobile node (MN) to move seamlessly and securely from one point of attachment (PoA) to another. Several network (L3) and application layer (L5) mobility protocols (Mobile IPv4 [1], Mobile IPv6[2] and SIP-M[3]) have been developed that try and maintain a seamless communication when the mobile performs a handoff. These protocols however need some additional optimization techniques at various layers to augment their efficiency. Although there are several optimized and expedited variants of these protocols such as FMIPv6 [4], MPA (Media Independent Pre-Authentication) [5] is a set of techniques and signaling mechanisms that assists such existing mobility protocols in providing such fast proactive handoffs. It does so by way of pre-authentication, pre-configuration and proactive binding update with the target network. This way, the MN does not need to reconfigure its network and link associations or configurations after moving to the target network. Traditionally, a MN decides to handoff to a new network based on the signal-to-noise ratio of the neighboring network. However, many modern mobile wireless devices are equipped with Global Positioning System (GPS) service provided by the vendors and service provides. Location-based services, GPS-based routing [6] and GPS-assisted handoff [7] are some of the common mechanisms that can take advantage of the MN's GPS coordinates. GPS co-ordinates can also be used to discover the relative location of the MN with respect to the neighboring networks. Thus, GPS co-ordinates of the MN can also help augment the existing MPA scheme to provide fast-handover. Till now the decision making for handover has been done based on the received power at the MN from the current PoA. We perform an alternative decision making criteria based on indoor ''Pseudo'' GPS co-ordinates of the MN.

Thus we can summarize our contributions as follows:

- Study of location-based co-ordinates as a criterion for performing proactive handoff
- A comparison of the various handoff related metrics based on SNR and Pseudo GPS co-ordinates

The remainder of the paper is organized as follows. We describe some of the related work in Section II that take advantage of the MN's coordinates to perform proactive handoff. We provide an overview of the 802.11-based Keaau Location Tracking System [8] in Section III. Section IV describes how Media Independent Handover can be integrated with the Keaau location tracking system. We highlight the functional components of the testbed and demonstrate the empirical results for real-time multimedia communication using the proposed location information based proactive handover. Finally, Section VI concludes the paper.

II. Related Work

The importance of location based handoff techniques is well understood. Wang and Wu [8] discuss how a combination of location information and SNR can provide better performance by reducing unnecessary handoff. Tom Van Leaden et al [9] discuss how a protocol assisted by location information from a vehicle can predict the handoff (thereby enhancing the overall handoff performance). Julian Mention and Thomas Noel [10] describe an experimental system that demonstrates how handover performance is improved by using Geo-Location Information provided by a GPS system. They suggest using MIPv6 in combination with GPS coordinates to provide fast-handoff. However there has been no consideration for any kind of the pre-authentication support, essential for inter-domain handover. In this paper, we provide a comprehensive handover solution that takes into account the inter-domain handover. It integrates pre-authentication support with indoor location tracking system that provides a means for proactive handover decisions.

1930-529X/07/$25.00 ©2007 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

III. Overview of the Location-based system

A. Overview of MPA

MPA [5] is a mobile-assisted higher-layer authentication, authorization and handover scheme that is performed prior to establishing layer 2 associations to a network (where mobile may move in near future). It provides a secure and seamless mobility optimization that works for inter-domain handover and heterogeneous handover involving both single interface and multiple interfaces. MPA is a set of techniques and algorithms that are executed to ensure seamless handover and connectivity to the target network by performing pre-configuration and pre-authentication to the target network before the actual handover takes place. It can be used to enhance the performance of existing mobility protocols by performing the proactive layer 3 and layer 4 associations and bindings before the actual handover actually takes place, thereby saving time for these operations that usually take place after the layer 2 association. Even the layer 2 handover is enhanced by suppressing the 802.11 AP channel scanning and best AP selection at the interface driver by having prior information of the channel number of the selected target network SSID (done for the sake of a proof of concept). So association to the target network avoids channel scanning, detection of the PoA MAC address and appropriate channel selection.

Figure 1 briefly demonstrates different functional components that are part of media independent pre-authentication and provide proactive pre-authentication, pre-configuration and proactive handover tunneling techniques. Details of these functional components and their operation can be found in reference [5].

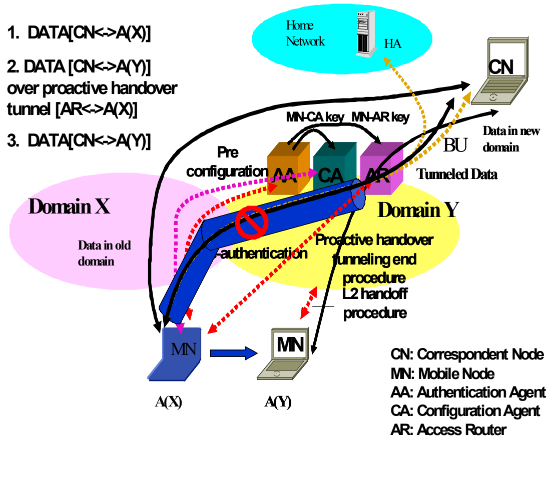


Figure 1: Basics of MPA Operation

B. *802.11 Based Location Tracking / Positioning System*

We have used 802.11-based Ekahau Positioning and Location Tracking Systems for our experiment. Ekahau is 802.11 based location estimation system [8]. Currently it is used extensively for tracking medical representatives and devices within hospitals. In our experiment, we are using this system to track the location of the MN. The system consists of Ekahau Positioning Engine (EPE), an Ekahau Client (which is tracked by the Ekahau Positioning Engine) and the Ekahau Manager (a GUI interface to show visibly the location of the nodes being tracked on the map). For tracking the location of Ekahau Clients, the server (EPE) first needs to perform a site survey (EPE Calibration) to determine the RSSI lists of the 802.11 beacons of all APs (Access Points) at several locations within the area of study. These RSSI lists from various locations are stored in an internal database within the EPE. During the site survey process, an Ekahau Client does an active scan of 1 through 11 channels and determines the existing 802.11 APs in the neighborhood and creates an RSSI list. The mobile sends this information to the EPE who in turn is able to determine the location of the Ekahau Client. The functional components of the Ekahau system are represented in Figure 2. For a detailed description of the system, the reader is encouraged to read the Ekahau Positioning System developers guide [11].

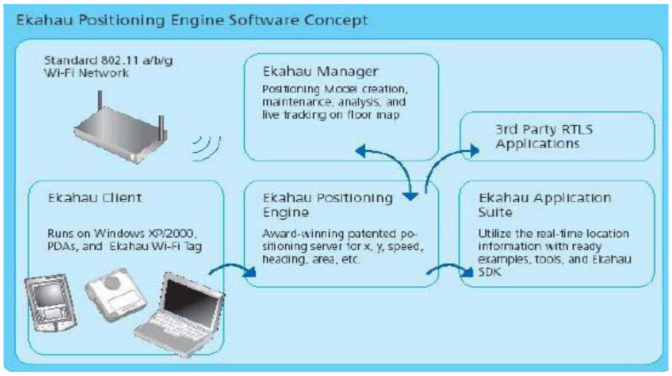
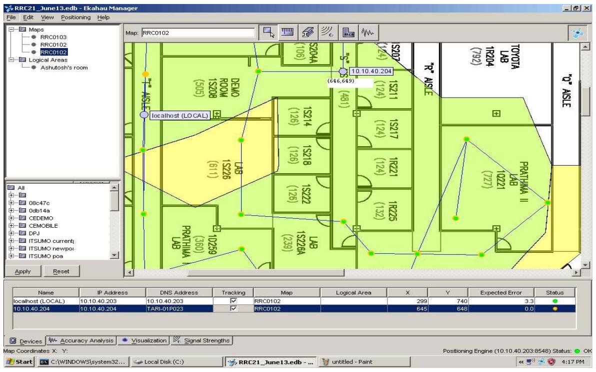

Ekahau Positioning Engine Software Concept
Standard 802.11 a/b/g Wi-Fi Network
Ekahau Manager
Positioning Model creation, maintenance, analysis, and live tracking on floor map
3rd Party RTLS Applications
Ekahau Client
Runs on Windows XP/2000, PDAs, and Ekahau Wi-Fi Tag
Ekahau Positioning Engine
Award-winning patented positioning server for x, y, speed, heading, area, etc.
Ekahau Application Suite
Utilize the real-time location information with ready examples, tools, and Ekahau SDK

Figure 2: Components of Ekahau Positioning System

Figure 3 shows the sample map of the area where the experiment was conducted. This map was created by taking SNR measurements of the existing APs in the neighborhood at some selected points.



Name	IP Address	DNS Address	Tracking	Map	Logical Area	X	Y	Expected Error	Status
localhost (LOCAL)	10.10.40.203	10.10.40.203	☑	RRC0102		299	740	3.3	●
10.10.40.204	10.10.40.204	TARI-01P023	☑	RRC0102		645	648	0.0	●

Figure 3: Location Survey using Ekahau

1930-529X/07/$25.00 ©2007 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

However, Ekahau system provides the ability to choose a selected set of APs to determine its own position during the handoff process.

IV. Location Assisted MPA

There are a few advantages of using a location-based system for handoff related decision compared to a purely SNR dependent decisions:

- SNR is an unreliable metric as it varies significantly due to Free space fading, Multipath fading, and Rayleigh fading.

- SNR is not a useful or reliable metric in situations where there are a lot of users. It only helps in the selection of alternative APs with less number of users.

- In future, GPS assisted handover can be used. A cell can be based on an approximate logical area based on cell coordinates.

In this section, we describe the details of the systems dynamics associated with location assisted MPA. The Ekahau location tracking system is equipped with a Java client SDK that is used by the MN to make the pre-authentication and associated handoff decision. Currently, a Java program is being used to start the pre-authentication and perform the handover decision based on the coordinates of the mobile node. To determine the MN's co-ordinates, the Keaau WiFi Tag running the Ekahau Embedded Linux Client is mounted on the MN (which is periodically tracked by the EPE). A Java program running on the MN (using the client SDK provided by the vendor) is used to connect to the EPE and determine the location (coordinates) of the WiFi Tag. Thus, the mobile constantly tracks its own coordinates. Since the coordinates of the APs are also determined beforehand, the mobile can determine its own location relative to the APs that are in its neighborhood.

A. Pre-Authentication and Proactive Handover

Though the decision making process can be an extremely complicated process, since it involves factors such as received SNR from the current PoA and target PoA, position for the BS of the target network , local network administrative policies, we have kept this decision making process relatively simple during the prototype development. We briefly describe the decision making process associated with the handover and related pre-authentication procedure.

- Each target network has an access point associated with it. Thus, each zone can be defined by a ''range'' of coordinates relative to the access point.
- Based on the relative distance between the mobile and the possible access points, the mobile can determine its own position.
- As long as the mobile has not moved from its current position, it does not initiate the process of discovering any new network in the neighborhood.
- As the mobile observes a change in its own coordinates, it starts the discovery process by calculating its coordinate relative to neighboring access points.
- Thus, at any point of time the mobile knows if it is within the home network ''range'' or has moved out.
- If MN has moved from its original position but is within the Home Network then pre-authentication to all possible target networks is performed and the tunnels are created to all the possible networks through the existing wireless interface.
- Depending upon the mobility protocol (e.g., MIP or SIPM), binding updates are sent to the HA or CN.
- Once the MN has moved out of the Home Network, and is closer to one of the target networks it initiates the handover to the target network and deletes all the other existing tunnels that were created with other neighboring networks. Figure 4 depicts this specific scenario and illustrates other MPA-based components.

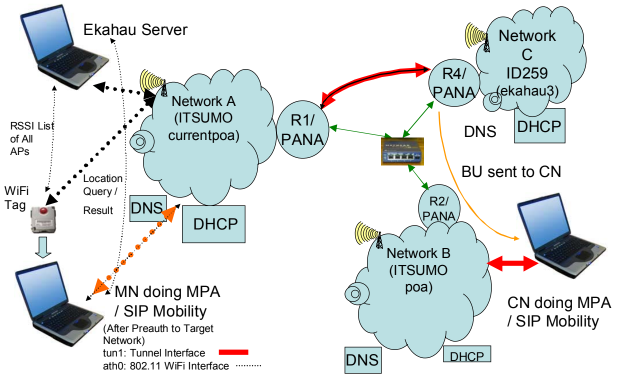

Ekahau Server
RSSI List of All APs
WiFi Tag
Location Query / Result
Network A (ITSUMO currentpoa)
DNS
DHCP
R1/ PANA
R4/ PANA
Network C ID259 (ekahau3)
DNS
DHCP
BU sent to CN
R2/ PANA
Network B (ITSUMO poa)
DNS
DHCP
MN doing MPA / SIP Mobility
(After Preauth to Target Network)
tun1: Tunnel Interface
ath0: 802.11 WiFi Interface
CN doing MPA / SIP Mobility

Figure 4 – Functional components of Ekahau assisted MPA

B. Types of Pre-authentication

Pre-authentication process with multiple candidate target networks can happen in several ways. We provide the highlights of multiple pre-authentication process.

The very basic scheme involves authenticating the MN with the multiple authentication agents in the neighboring networks, but actual pre-configuration and binding update take place only after layer 2 movement to a specific network is complete. By having the pre-authentication done in advance, the MN does not require to authenticate any more after it moves to the new target network. Configuration and binding updates actually take place after the mobile has moved to the new network and thus may contribute to the delay.

Similarly, in addition to pre-authentication, the MN can pre-configure, while in the previous network, to new networks' configuration(s), but can postpone the binding update until after the MN has actually moved within the ‘‘range’’ of the new network. The MN may obtain multiple IP addresses from the neighboring networks ahead of time, but stores these in a cache. This can potentially reduce the latency of acquiring new IP address (about ~ 2 sec. for DHCP). Like the previous case, in this case the MN also does not need to set up the pre-configured tunnels. While pre-authentication process and part of pre-configuration process are taken care of before the MN has moved to the new network, binding update is actually done after the mobile has moved.

The third type of multiple pre-authentication involves all the three steps while the MN is in the previous networks, such as authentication, configuration and binding update. But, this specific process utilizes the maximum amount of resources. Some of the resources that get used during this process are as follows:

1) Additional signaling for pre-authentication in the neighboring networks

2) Keeping the IP address of the neighboring networks in MN’s cache for certain amount of time. It needs additional processing in the MN for storing these IP addresses. In addition, it also uses up the temporary IP addresses from the neighboring routers.

3) There is an additional cost associated with setting up additional transient tunnels with the target routers in the neighboring networks and mobile.

4) In case of binding update with multiple IP addresses obtained from the neighboring networks, multiple transient streams flow between the CN and mobile using these transient tunnels.

When only pre-authentication and pre-configuration are done ahead of time with multiple networks, the mobile sends one binding update to the CN. In this case it is important to find out when to send the binding update after the layer 2 handoff.

In case binding update with multiple contact addresses is sent, multiple media streams are sent by the CN using the transient tunnels. But in that case one needs to send another Binding Update after the handover with the contact address set to the new address (only one address) where the mobile has moved. This way, the mobile stops sending media to other neighboring networks where the mobile did not move.

The pre-authentication and handover decisions can be made more complex. The pre-authentication can be done in the overlapping regions of two or more networks, so as to avoid unnecessary usage of resources and processing time. However, the pre-authentication process being costly (time complexity of the process is high), we avoid doing it in the overlapping region of two networks (the overlapping region being small). Moreover, there is no well defined ‘‘physical boundary’’ separating two regions (area of coverage). The EPE supports logical demarcation of co-ordinates as logical area boundaries. The Java SDK can be used to connect to the EPE to obtain these logical area updates. However, we observed very erratic results possible due to the inaccurate RSSI update (which is based on received SNR from 802.11 beacon frames of all APs within the WiFi Tag’s correct reception range) the WiFi tag reports to the server

In a more complete scenario, the MN sends a query to the *Application Information Service (AIS) [11]*. The query includes the current coordinates of the mobile node and then the mobile obtains the coordinates of the neighboring networks. After receiving these information the mobile makes the Pre-authentication and handover decision. This location information is simply used to update an XML configuration file on the MN which then triggers the Pre authentication and makes the handover to the target network(s).

Figure 5 describes different network elements of the target networks that are used in the testbed during multiple pre-authentication. In this scenario, the mobile is doing pre-authentication to all the target networks.

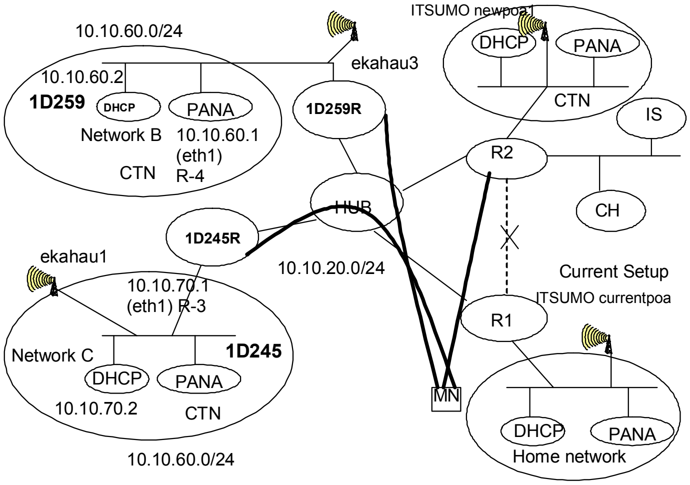


Figure 5: Multiple Pre-authentication Experimental Testbed

V. Analysis of Experimental Results

We provide the details of some of the functional components that are used in the testbed. We have used Fedora Core 5 Distribution running Linux Kernel 2.6.12 on the routers, MNs, and correspondent nodes (CN). We used PANA and Open Diameter for the local authentication and AAA support respectively. DHCP server was used to configure the Layer 3 identifier of the mobile. We have configured the Linux laptops with “hostap” drivers so that these could behave as Access Points. The MN has a Netgear Atheros 802.11 WG511T interface card which is supported by the Linux MadWiFi driver. The driver is especially modified to avoid scanning of all channels. Based on the target network selected and the ESSID of the target network selected, the driver avoids the scanning of all 1 through 11 channels and associates only to a particular channel number which is channel number of the target PoA. Thus when the ‘iwconfig’ program is executed for the particular target network, the MAC address and the channel number of the target network PoA are known in advance. Thus the driver avoids scanning and associates directly to the target network. In this specific experiment we have used SIP-based mobility as the mobility protocol [3] and thus use the binding update to the corresponding node.

The client first registers itself as a valid client to the EPE and queries it for WiFi Tag – a device whose IP address is presented to the server. The server reports back with the signal quality and status of the WiFi Tag as seen by the server. Thereby the server sends Location (Coordinate) updates from time to time to the client. The client implements a Location-Estimate-Listener interface to retrieve the location (X, Y) of the WiFi Tag and thereby based on the location makes the decision to do the pre-authentication or handover to the target network. Our current prototype tests the performance of real time applications such as VoIP. It uses MPA techniques and client location to do pre-authentication and pre configuration to the target network in a proactive manner. We compare both the results; the one obtained by location information update using Ekahau positioning engine with that of obtained using SNR. Table 1 shows the results obtained using the location update using Ekahau-based location tracking system. Table 2 shows the results obtained using SNR. Average inter-packet gap is different in each of these cases as a different codec was used for each case.

Table 1: Handoff triggered by the location of the mobile

Handoff Parameters	Buffering Enabled SIP-Mobility	Buffering Disabled SIP- Mobility
L2 Handoff (ms)	6.0	6.0
Avg. packet loss	0.0	2.0
Avg. inter-packet gap (ms)	60.0	60.0
Avg. inter-packet gap during handover (ms)	65.0	60.0
Buffering period (ms)	40.0	n/a

Table 2: Handoff triggered by SNR of the client

Handoff Parameters	Buffering Enabled SIP-Mobility	Buffering Disabled SIP- Mobility
L2 Handoff (ms)	4.0	5.0
Avg. packet loss	0.0	1.5
Avg. inter-packet gap (ms)	16.0	16.0
Avg. inter-packet gap during handover (ms)	n/a	29.0
Buffering period (ms)	20.0	n/a

In both the cases we have used SIP as the mobility protocol, and have included the results for both buffering and no-buffering cases. It is interesting to learn that results obtained from both of these experiments it exhibits similar performance when used in conjunction with pre-authentication. On the other hand, a location-based handoff scheme is more suitable for a highly mobile environment. In some cases, a combination of SNR and location-based handoff technique maybe more desirable. During the experiment, we observed some inaccuracies in location estimation by the Ekahau system due to constantly varying SNR of the 802.11 APs at the WiFi TAG and inaccurate logical area probability updates.

VI. Conclusions

Although signal-to-noise ratio is commonly used to determine the handoff between the networks, handoff based on only SNR may give rise to ping-pong effect that ultimately degrades the overall handoff performance. Handoff can also be triggered based on the location of the mobile. Results from our experimental analysis based on an emulated GPS-based coordinates demonstrate that one can achieve the results that are comparable to SNR-based approach and at the same time this technique could be more applicable in a highly mobile environment. Thus, a handoff algorithm based on a combination of relative location of the mobile and the signal-to-noise ratio will increase the probability of successful handoff without compromising the delay and packet loss performance. Based on the type of environment mobile is operating on, it maybe desirable to choose either one of these techniques or a combination.

References:

1. C. Perkins et al, Mobile IPv4, RFC 3344, IETF, August 2002
2. D. Johnson et al, Mobile IPv6, RFC 3775, IETF, June 2004
3. H. Schulzrinne and E. Wedlund, “Application Layer Mobility using SIP,” pp 47-57, vol 4, issue 3, ACM MC2R , July 2000
4. R. Koodli (Ed.), "Fast Handovers for Mobile IPv6,” IETF RFC 4068, July 2005
5. A. Dutta (Ed.), “A Framework of Media-Independent Pre-Authentication,” draft-irtf-mobopts-mpa-framework-00, IRTF MOBOPTS RG, Work in progress, Aug 2007
6. T. Imielinski and J. C. Navas, “GPS-based geographic addressing, routing and resource discovery,” Communications of the ACM, volume 42, issue 4, 1999
7. A. Dutta et al, “GPS assisted fast-handoff for Real-time communication,” IEEE Sarnoff Symposium 2006, Princeton
8. Peter Wang and Chih-Hao Wu, “Effective Handoff Method using Mobile Location Information,” IEEE Vehicular Technology Conference, 2001, Atlantic City, NJ
9. Tom Van Leaden et al, “ Location Assisted Fast Vertical Handover for UMTS/WLAN Overlay Networks,” Springer Lecture Notes in Computer Science, 2005
10. Julian Mention and Thomas Noel, “IEEE 802.11 Handovers Assisted by GPS Information,” IEEE Womb 2006, Montreal, Canada
11. Keaau System Manual, http://www.ekahau.com
12. IEEE P802.21/D04.00: Draft IEEE Standard for LAN/MAN: Media Independent Handover Services February, 2007