11-30-2010

A Proposed Policy-Based Management Architecture for Wireless Clients Operating in a Heterogeneous Mobile Environment

Mayank Keshariya
University of Canterbury

Ray Hunt
University of Canterbury

DOI: 10.4225/75/57b670bb3477d
8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

A Proposed Policy-Based Management Architecture for Wireless Clients Operating in a Heterogeneous Mobile Environment

Mayank Keshariya and Ray Hunt
Computer Security and Forensics Group
Department of Computer Science and Software Engineering,
University of Canterbury
Christchurch, New Zealand
mayank.keshariya@canterbury.ac.nz
ray.hunt@canterbury.ac.nz

Abstract

The objective of this paper is to provide a managed always best connected service to mobile entities over underlying heterogeneous wireless and mobile platforms while maintaining negotiated security and quality of service (QoS). This paper proposes a new model and its architecture which is based upon Policy-based Management but provides a new framework based on layered-approach for the centralised management of mobile clients. In particular, we propose and implement a new model of a policy-managed mobile client and its architecture to support seamless handoff across multiple access networks. The proposed mobile client supports multi-domain authentication, authorisation and security based on user profiles as well as the ability to negotiate management services over interconnected heterogeneous mobile platforms. We have also proposed a new handoff initiation algorithm to select an optimum time to handoff. This algorithm combines metrics in a novel way using standard deviations without resorting to other computationally intensive methods. Finally, this paper describes a proof-of-concept implementation based upon Microsoft Windows presenting a performance analysis to validate our architectural approach.

Keywords

Policy Based Management, heterogeneous networks, mobile clients, always best connected, optimum handoff, network selection algorithm.

INTRODUCTION

There have been many changes in the face of computing in the past decade, one of which is undoubtedly the introduction of mobile computing. With an increasing number of wireless hotspots, cellular networks and featured mobile devices, mobile computing has become widely accepted as a useful and dependent productivity tool.

Since no single technology, service or infrastructure can provide ubiquitous coverage and high throughput across all geographical areas, the current industrial trend is towards merging existing communications technologies (such as email, Video on Demand, Voice over IP), with new access technologies (such as WiFi, Digital Subscriber Line, 3G), as well as device control, to offer greater mobility.

Additionally, these access technologies vary in bandwidth, delay, communication range, power consumption, security, reliability, end-to-end cost, end-user preferences and various other aspects [Frodigh, 2008]. There is a consensus that the next generation of access networks will consist of a set of partially overlapping heterogeneous networks [Lu, 2002], where service providers will offer access to their network via different technologies (Figure 1). The existence of multiple access networks will offer new wireless services where these technologies and networks can coexist in a complementary manner to allow users to be always connected by seamlessly switching between them irrespective of their mobile-networked device, preferred access technology or the service provider.

BACKGROUND TO POLICY MANAGEMENT IN A MOBILE ENVIRONMENT

The primary issue in offering always connected services is that although overlapping, different access networks are not particularly integrated and hence users, in most cases, are forced to manually perform the switch between networks, service providers or access technologies. This may include reconfiguring their mobile devices to select a particular technology (e.g. 3G to WiFi) together with inputting the security credentials for the new network, restarting running applications, and if required, manually adjusting bandwidth utilisation.

Handoff and Mobile IP

To address this issue, the IETF mobileip Working Group has standardised the Mobile IP protocol [Perkins, 2002] to perform a handoff by extending the Layer-3 (IP layer). A handoff is a process by which the ongoing communications and current sessions of a mobile device is transferred from one point of a connection in a network to another point of connection in the same or different network.

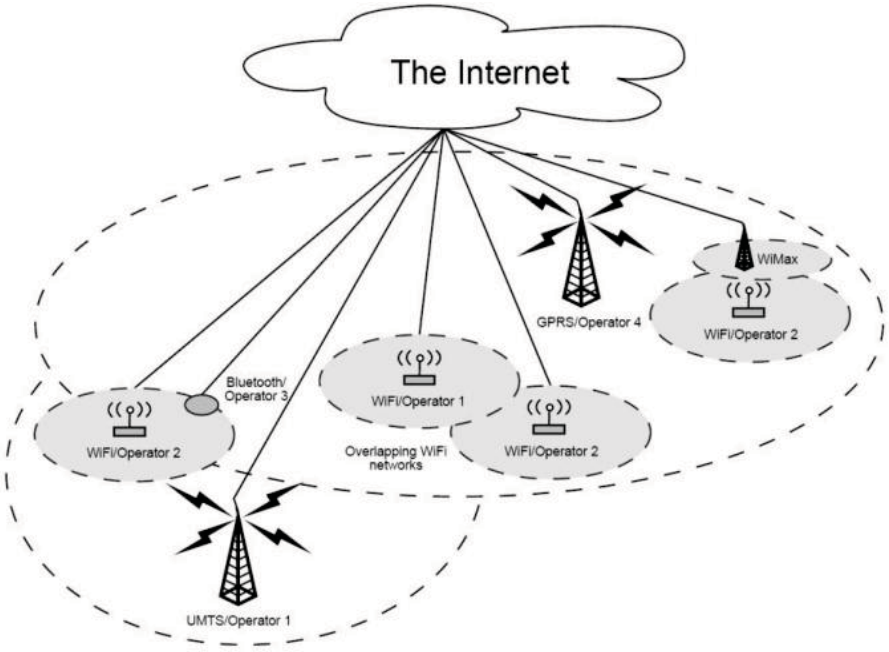

Figure 1: Overview of heterogeneous networks

Hence, any handoff procedure involves a set of protocols to notify all the related entities of a connection that a handoff has been performed, and that the connection has to be redefined. During or immediately after a handoff, it is common that packet losses and delay occur due to signalling and location updates which results in effecting users' current ongoing communications. Furthermore, it involves a sequence of events in the service provider network, including rerouting and reregistering the connection, which puts additional load on the network traffic. Hence handoff performance is a critical issue.

On the other hand, to realise the mobility requirements of a mobile user and the mobile device (collectively termed as a mobile entity), a service provider needs to authenticate and authorise the mobile entity (i.e. the user and/or the device). This requires service providers to be able to dynamically manage their resources, to be able to perform authentication and authorisation checks and, if required, be able to negotiate acceptable service levels with other service providers and the mobile entity to continually provide agreed services. Hence, offering always best connected services requires support from both service providers and the mobile entity.

Policy Based Management System

While defining a handoff procedure, the Mobile IP protocol, however, does not address issues from the service provider side which require a centralised management system to administer their networks and be able to provide an acceptable service to their current users and any *roaming* mobile entity.

Policy-Based Management (PBM) has emerged as a promising solution for a centralised management of networks and distributed system [Strassner, 2004]. PBM aims to provide system administrators with a centralised administration window to define rules based on business-level policies. The policy framework within the PBM then translates these policies into configuration rules/commands and implements them across the network (Figure 2).

The PBM has identified two main components: a Policy Decision Point (PDP), which, based on a set of business policies and current network conditions, decides which policy to implement, and a Policy Enforcement Point (PEP) which implements the high-level policy as device specific commands. Hence, to employ a PBM approach to provide always best connected services, a PEP is required in a mobile node.

A PBM system can be defined as a subset of the Information Management System which is defined as a set of policies to maintain a set of processes to manage information assets. In the case of PBM, the assets are: bandwidth resources, maximum number of allowed connections and service level of current connections.

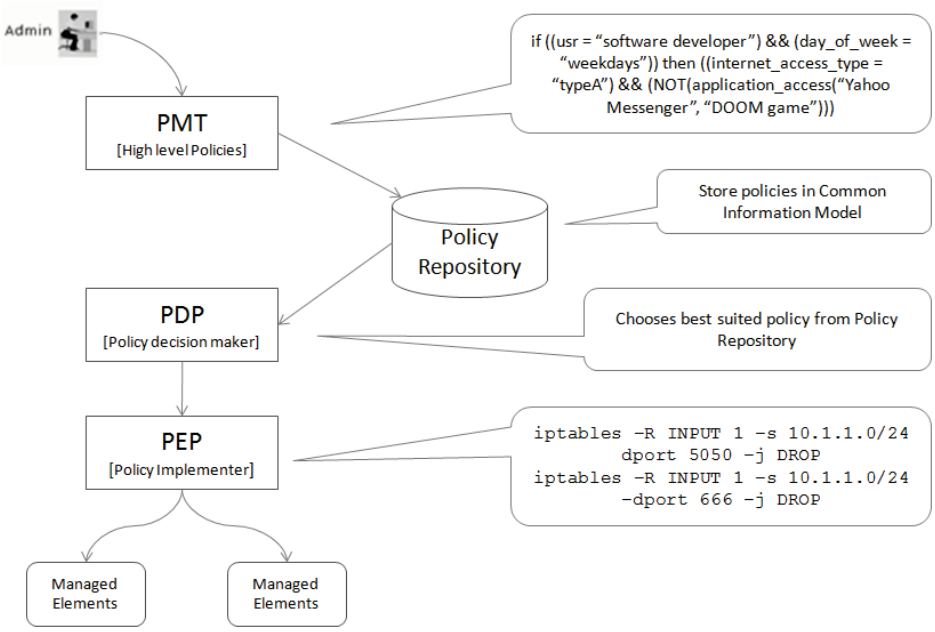

Figure 2: Overview of Policy-Based Management system

DESIGN OF THE MOBILE CLIENT MODEL

As discussed in Section 2, the main requirement of being always connected is to perform a transparent handoff which requires support from both the network and client. The Mobile IP protocol, although providing handoff does not cater for requirements of network side where a PBM system is required to be supported by the service providers. This means that the mobile client should implement a component similar to the Policy Enforcement Point described above, which can put into action the high-level policies as device-specific commands, and if necessary, should be able to negotiate the offered services with the service provider.

Additionally, since any handoff procedure introduces message exchanges, location updates and additional load on the network, it should be performed only when required. The Mobile IP protocol while addressing *how-to* perform a handoff, does not address *when-to* perform such a handoff.

Requirements of a Policy-Managed Mobile Client

We have identified the following set of requirements which *must* be addressed by a framework to provide an always connected service to the mobile entity:

i. *Transparent handoff*

   The handoff should be *seamless* with minimal effect on the current sessions by minimising the number of dropped packets. The handoff should also be *transparent* with minimal intervention from the user.

ii. *Optimum selection of network and interface*

   The framework should be able to detect, monitor and choose the current or other available access networks and interfaces.

iii. *Optimum time to handoff*

   The framework should be able to detect whether a handoff is required to the *best* available network/interface and select an optimum time to handoff with an attempt to minimise the number of handoffs.

iv. *Support for protocols*

   The framework should be able to support a range of protocols of the services to be offered to the mobile entity including Mobile IP for mobility, Radius/PPTP for authentication, WPA/802.1x for security in the data link layer and IPSec/VPN support for security in the IP layer. For example, to support multimedia communication sessions

such as voice and video over the Internet, the framework needs to support protocols such as the Session Initiation Protocol (SIP).

v. Support for profile

The framework should support a profile-based system to interact with the PBM system of the service provider. This framework should implement a PEP component which can interact with the PDP of the service provider's PBM system. The profile can be handled manually within the mobile device, or if the service provider implements a compatible PBM system, then the profile may also be downloaded from the service provider directly into the mobile device.

We have identified two further types of profile:

- An *internal profile* which manages information with respect to the personal preferences of the user (e.g. priority of access networks based on bandwidth, services, cost, type of applications), security profile for different locations (e.g. connecting from home to work requires a secured Virtual Private Network) and authentication information (e.g. connecting to an office network requires a digital certificate).
- An *external profile* is supported by the service provider and contains the role and status of the mobile user (e.g. gold user of a cellular network).

Depending on profile information, the framework can control the behaviour of the mobile entity and communicate with the service provider.

PROPOSED POLICY-MANAGED MOBILE CLIENT MODEL

Based on the requirements identified in Section 3.1, we propose a new model for a policy-managed mobile client. We have defined the management framework (Figure 3) as a four-layer stack: Policy Layer, Mobility Layer, Enforcement Layer and Network Layer.

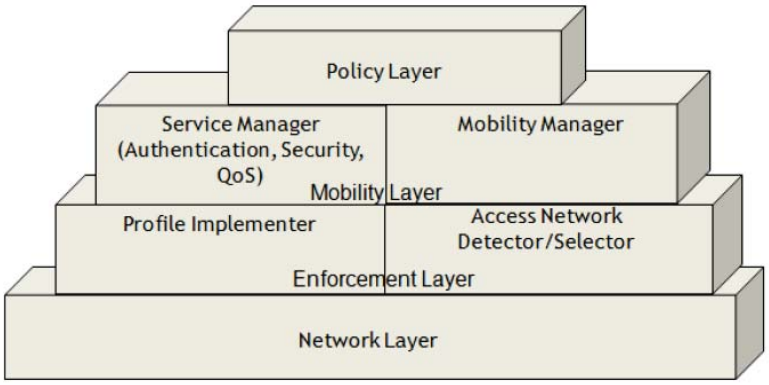

Figure 3: Proposed Model of Policy Managed Mobile Client

a. The *Policy layer* provides support for profile management and manages the profiles downloaded from external sources (e.g. service providers). We have also introduced a new Infrastructure (I) parameter to ensure whether the offered infrastructure from the service provider is acceptable to the mobile entity. This then assists the mobile device to behave in accordance with the user's profile and network's present service conditions (discussed in Section 3.3).
b. The *Mobility layer* provides seamless and transparent mobility to the mobile entity. It contains a set of *managers* to manage a set of protocols which are used to offer a set of services. The Mobility layer contains two main components (i) the Mobility manager, which manages the mobility protocols (such as Mobile-IP for IPv4 or IPv6) and maintains current sessions when the mobile device is in the state of handoff between access networks, and (ii) the Service manager which supports the services for a mobile entity including parameters for providing authentication, security, QoS, Voice over IP, Video over IP, etc.
c. The *Enforcement layer* implements the *internal* and *external* profiles (Section 3.1). We have identified two main components: (i) Profile implementer which supports the downloading of high-level profiles from the ISP as well as device relevant information, and (ii) Access Network Detector/Selector component, which incorporates network detection and optimum time selection algorithms which continually monitors available access networks selecting the best time and access network to which to perform a handoff.
d. The *Network layer* functions in accordance with the decisions of the Policy Implementer by implementing profile-based policies into low-level device-specific commands. The command interpretation is specific to the mobile device. The Network layer directly interacts with the network interfaces (wireless radio) and is dependent on the device drivers of various notebook, netbook, handheld and mobile devices running different operating systems such as

Microsoft Windows, Apple Mac OS, Linux, Symbian, iOS, WebOS, Android, Windows Mobile, etc. Further comparison with and pointers for further research involving these operating systems are discussed in Section 5.3.

Infrastructure Parameter

We have introduced an Infrastructure (I) parameter to validate whether the offered infrastructure support from the service provider is acceptable to the mobile entity. For example, while connecting to a wireless hotspot, a user's internal policy may require at least WEP security along with IPSec-VPN tunnel support. If the new service provider does not offer this service or features, the user may not accept the connection.

However, while using the Infrastructure parameter, there are no explicit message exchanges between the service provider and the mobile entity. Simply stated, it is a Boolean value deciding whether the available *best* connection should be accepted by the mobile entity based on the current offerings of the service providers after reference to the internal and external profiles. This combination approach of handoff algorithm combined with user preferences provides a method by which the mobile user has finer control over the entire handoff process.

PROPOSED ARCHITECTURE

Figure 4 presents the architectural framework of the proposed model discussed in Section 3.2. To demonstrate the working of the architectural components, we will illustrate by way of a real-world scenario where a ubiquitous coverage of 3G services is available and is provided by *3GNZ*[1] service provider. A set of hotspot areas are available, where WLAN services are provided by the *WiFiNZ* service provider. We assume that there is no service level agreement (SLA) between respective companies and a mobile user is required to purchase separate subscriptions. We also assume that each service provider maintains a PBM system and is able to honour the SLA with their users.

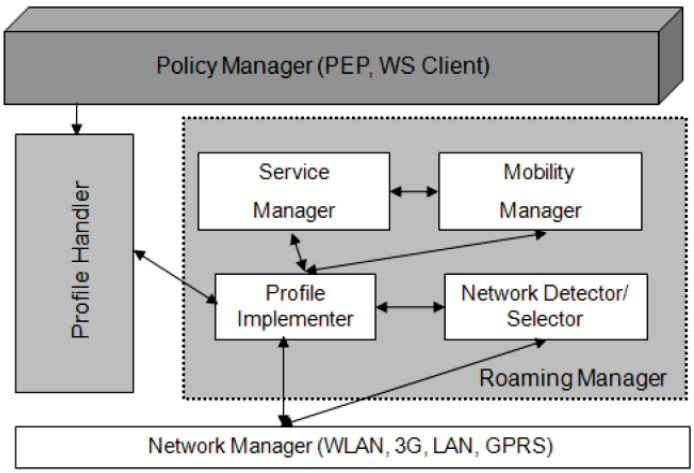

Figure 4: Proposed architecture of Policy Managed Mobile Client

Consider a scenario where a mobile user *John* works in a company *ABC* which supports the Mobile-IP protocol. Every mobile user is required to initiate a secured VPN connection to connect to the company's internal servers. *John* has a notebook computer equipped with WiFi and 3G wireless cards and has the proposed policy managed mobile client installed as a software module.

The working of the proposed architecture will be as follows:

0. The *Policy Manager* allows the mobile user (*John*) to add his preferences, such as priority of individual access devices, related costs based on purchased subscriptions, support for applications, etc, and stores them as an internal profile. These profiles are transferred to the *Profile Handler,* which maintains a local schema of such information.
1. When the mobile node starts, the *Roaming Manager* initiates *Profile Implementer* and *Network Detector/Selector* modules. The Profile Implementer then downloads the profiles.

[1] Hypothetical organizational and client names are used to illustrate the applied and practical nature of this proposed model

2. The *Network Manager* prepares a list of active interfaces (i.e. WLAN and 3G in this case) and starts scanning the availability of respective services. This information is forwarded to the Profile Implementer which detects whether the mobile node is in the home network or not based on the current IP address(es) of its network interfaces.
3. If the mobile node is away from the home network and there are more than two access networks available, the Profile Implementer then forwards the device information together with the profiles to the Network Detector/Selector module.
4. Assuming that current networks available are WLAN (*WiFiNZ*) and 3G (*3GNZ)*, the Network Detector/Selector selects the best applicable network device (i.e. *WiFiNZ*) and access network (*3GNZ*) and informs the Profile Implementer.
5. The Profile Implementer then initiates the *Mobility Manager* for Mobile-IP and *Service Manager* to create an IPSec-based VPN tunnel from the mobile device to the *ABC*'s PBM system.
6. The Network Detector/Selector module continues to monitor the network parameters to identify the need for handoff. In the case where a handoff is required, the Profile Implementer is informed to initiate a Mobile-IP registration request.

COMPONENTS OF THE PROPOSED ARCHITECTURE

This section presents a brief overview of each component introduced in the proposed architecture:

a. The *Policy Manager*, which acts as a PEP, downloads and stores the user profile from its home network. The communication may be based on direct implementation of PBM such as the COPS (Common Open Policy Service) protocol [Boutaba and Polyrakis, 2002] or a generic XML-based Web Services implementation [He et al, 2004] which can also be used in negotiating services between a mobile entity and the service provider. A profile essentially identifies the class of service to which the user is registered and refers to the SLA between the user and the service provider.

b. The *Roaming Manager* is a composite component to provide mobility, security and QoS, to the mobile entity by selecting and connecting to the best available access interface. As the handoff decisions and handoff operations are performed at the mobile node, the Roaming Manager periodically collects current network conditions to analyse for the most appropriate network(s). The Roaming Manager consists of Mobility Manager, Service Manager, Profile Implementer and Network Selector/Detector modules, viz.:

   i. The *Mobility Manager* handles the mobility protocol, such as Mobile IPv4 or IPv6, which involves processes such as routing table manipulation, location updates and packet encapsulation. It also performs the re-routing of packets during any handoff and sending registration requests to the home network.

   ii. The *Service Manager* provides a framework to support all the protocols of the services being offered to the mobile user. Additionally, it is tightly integrated with the Mobility Manager to support protocols for security, authentication and QoS. Table 2 provides a list of standard protocols which commonly need to be supported to offer respective services to the mobile client.

Requirements	IETF Standard Protocols
Authentication	Radius, Diameter, Kerberos, Domains
Security	802.1x, IPSec, VPN, SSL, EAP-TLS
Mobility	Mobile (IPv4, IPv6), Hierarchical MIP, TeleMIP, Cellular IP, Hawaii
Performance	QoS, Grade of Service, SLA
Improvements	IPv6, interoperability between heterogeneous networks (802.21)

Table 2: Protocol support by Service Manager

   iii. The *Profile Implementer* implements the internal and external profiles translating these to device specific information. It maintains both the statistical and abstract information of the profiles. The statistical information comprises measurable attributes such as received signal strength, perceived bandwidth, round trip time, etc, while abstract information is relative and is often based on a number of user and application dependent factors such as personal preferences, device capabilities, current active applications and their specific needs, current

sessions and their connectivity requirements, network resources, and network coverage. We have referred to them collectively as *user's current context*.

iv. The *Network Detector and Selector* module incorporates network detection and optimum network selection algorithm. We have also proposed a new network selection algorithm to be discussed in Section 4.2.2.

c. The *Profile Handler* interacts with all the components as a common message bus where abstract-level policies from the Policy Manager are forwarded to the Profile Implementer, which are then implemented by the Network Manager. Considering the limited processing and battery power of mobile devices, we assume that the policies are *conflict-free*. Since a profile is used to identify a priority among the network interfaces and devices, this assumption is relevant in real-world scenarios as well as in semantic analysis of policies, where one of the prominent conflict resolution techniques is achieved through prioritisation [Moffett and Sloman, 1994]. Figure 5 presents a sample of an internal profile stored in XML format.

```
<?xml version="1.0" encoding="UTF-8" ?>
<profile>
<name>internal profile</name>
<description>Personal preferences of user</description>
  <date>
    <from>090223</from>                    <!– 23-Feb-2009 -->
    <till>090628</till>                    <!– 28-Jun-2009 -->
  </date >
 <time>
    <from>000000</from>
    <till>235959</till>
 </time>
<interfacepriority id="interface"> <!– Interface priority list-->
          <level>Ethernet</level>
          <level>Wireless</level>
          <level>PPP</level>
</interfacepriority >
<networkpriority id="network">      <!– Network priority list-->
          <level>Ethernet</level>
          <level>UC wireless</level>
          <level>Costa A</level>
          <level>CDMA</level>
</networkpriority >
</profile>
```

Figure 5: Sample of an Internal Profile stored in XML format

d. The *Network Manager* translates and implements the policies into device specific commands. It is an architectural implementation of the Network Layer of the proposed model. The Network Manager maintains a direct communication with the network adapters of the mobile device and collects real-time information which is then used by the Network Detector and Selector module. The implementation of a Network Manager is specific to the internal hardware and device drivers of the mobile device.

MOBILITY BETWEEN HETEROGENEOUS NETWORKS

The traditional algorithms for selecting an optimum time to handoff usually employ simple intuitive rules to compare the received signal strength from different points of the connection and then decide on when to perform a handoff. However, the degradation of the signal level is a random process, and decisions based only on current signal strength may result in a *ping-pong effect*. A ping-pong effect is when a mobile device handoffs to the access network whose signal strength is higher in that instantaneous moment and initiates a series of handoffs when the signal strength is constantly fluctuating e.g. when a mobile node is moving on the perimeter of a WiFi network, hence degrading the overall service level [Feng and Reeves, 2004].

Handoff Initiation

Current research commonly focuses on either using the most obvious metrics (e.g. received signal strength, bit rate, etc.) [Stemm and Katz], or using advanced methods (such as Fuzzy logic, pattern recognition) which involves complex mathematical equations which demands more processing power than can normally be handled by most mobile devices [Tripathi, 1999].

Our proposed algorithm extends earlier work [Park, 2002] [Hunt and Keshariya, 2005] and uses the received signal strength (RSS), threshold levels (T), Hysteresis margin (H) and weighted priority (P) of respective interfaces to

select an active interface over a time period (η), where the samples are analysed based on their standard deviation. The priority of any interface is a numerical representation of factors such as network bandwidth, cost, overall throughput, network latency and reliability which are defined in an internal profile. The internal profile also includes user preferences, e.g. user may want to be connected to the cheapest network available regardless of QoS or coverage offered.

A standard deviation is a measure of the variability of a set of values. A low standard deviation indicates that the sample data points tend to be very close to the same value (i.e. the average of all the values) whereas high standard deviation indicates that the values of the data set are spread out over a large range of values. Hence, the use of standard deviation on a sample data collected over a time period portraits a near accurate representation of the present conditions.

Handoff is performed when new Connection Point (CP) has more weight than old CP i.e. $CP_{new} > CP_{old}$. The comparison includes following factors:

- RSS plus **Threshold:** the RSS of a new CP exceeds that of the current one and the signal strength of the current CP is below a threshold T (i.e. $if\ RSS_{new} > RSS_{old}\ and\ RSS_{old} < T$).
- RSS plus $Hysteresis$: RSS of a new CP is greater than that of the old CP by a hysteresis margin H (i.e. $if\ RSS_{new} > RSS_{old} + H$).
- $RSS, Hysteresis, and\ Threshold$: RSS of new CP exceeds that of the current CP by a $hysteresis\ margin\ H$ and the signal strength of the current CP is below a threshold T (i.e. $RSS_{new} > RSS_{old} + H\ and\ RSS_{old} < T$).
- $Priority$: the priority P of a new CP is higher than that of an old CP by a factor margin. A $weight\ \omega$ of individual interfaces is calculated until the number of samples is greater than as defined by the dwell timer.
- $Dwell\ Timer$: a timer value η is defined to collect the number of samples. A standard deviation is calculated on each weight w_i over a time period of η. If the weight of the interface i is still higher, then a handoff is performed.

The flowchart of the proposed algorithm is shown in Figure 6.

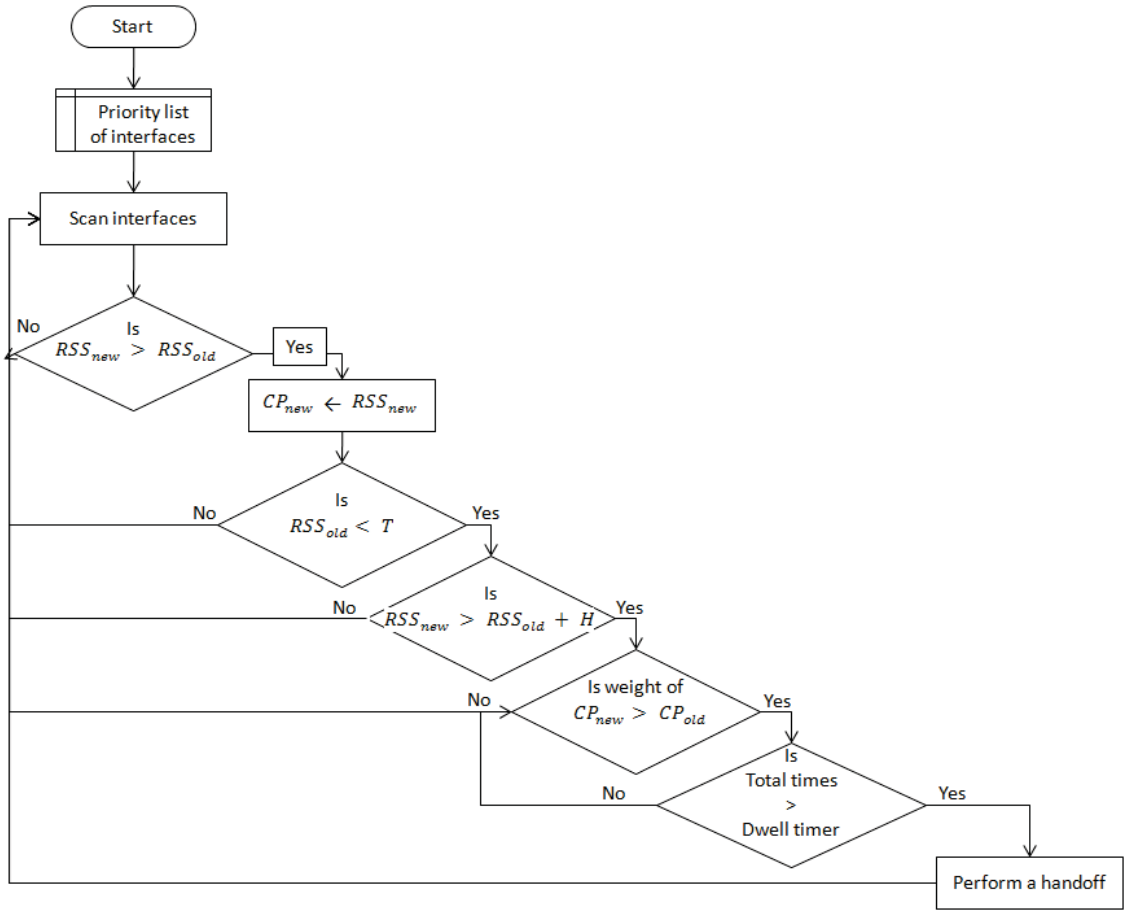

Figure 6: Proposed Network Selection Algorithm flowchart

Network Selection Algorithm

RSS is a measurement of the signal/noise ratio present in a received signal. However, the RSS values for different interfaces are different and cannot be compared directly. For instance, WiFi RSS is measured on –dB (negative

decibels) where lower value represents better connection and threshold values are between -40dB and -120dB, whereas 3G RSS is measured in +dB (positive decibels) and threshold varies between 15dB to 25dB. Hence, a normalised RSS is required for comparison.

The priority p_i is defined as a single numerical value of the set $\{1, 2, 3\}$. Mathematically, if parameters are defined as:

$$Normalized\ (s_i) = (s_i - L_i) / (H_i - L_i) * 100,\ for\ range\ [0,100]$$

$$RSS::\ s_i \in [0,100],$$

$$Priority::\ p_i \in \{1,2,3\}$$

$$Lower\ Threshold::\ L_i \in [0,100],$$

$$Higher\ Threshold::\ H_i \in [0,100],$$

$$Dwell\ Timer::\ \eta$$

Then the weight formula is derived as:

$$if\ i\ is\ the\ current\ interface, then$$

$$w_i = 1000 * p_i + 2s_i + H \quad if\ s \geq L_i$$

$$= 2s_i + H \quad if\ s_i < L_i$$

$$if\ i\ is\ not\ the\ current\ interface, then$$

$$w_i = 1000 * p_i + s_i - H \quad if\ s \geq H_i$$

$$= s_i - H \quad if\ s_i < H_i$$

$$\omega = \frac{1}{\eta}\sqrt{\left\{\eta\left(\sum_{i=1}^{\eta}(w_i{}^2)\right) - \left(\sum_{i=1}^{\eta}(w_i{}^2)\right)\right\}}$$

Perform a handoff when $\omega_{new} > \omega_{old}$

Analysis of proposed Network Selection Algorithm

The proposed network selection algorithm is novel since it employs the metrics in an optimal way with respect to the relevance of these metrics associated with the current context of the mobile user (i.e. available networks, speed of mobile user, active applications in a mobile device, user's personal preferences). Furthermore, our method uses conventional parameters such as received signal strength and additionally includes user's current context and weighted priority from their internal profile (based on their personal preferences). The algorithm then determines the standard deviation of these parameters employing delayed analysis (hysteresis effect) to determine if the handoff is still required.

The use of standard deviation is the key since it ensures that the mobile device has reached a stable state (i.e. well inside a hotspot area) before performing handoff. Also, mathematically, computing standard deviation requires less processing power considering we have ignored the round-off error, arithmetic overflow and arithmetic underflow to trade-off for the speed for performing calculations.

MULTI-DOMAIN AUTHENTICATION, SECURITY AND QOS

We have identified three different scenarios where the mobility requirements of a mobile entity changes: (i) when a mobile entity is connected to a managed PBM system as a guest user, (ii) when a mobile entity is connected without any supporting infrastructure i.e. current service provider does not have a PBM system and (iii) changes in the runtime requirements of applications currently running on the mobile device.

In the case of networks which are managed by a PBM system, they are no longer considered as a single entity providing basic connectivity, but can be treated as a service-enabling platform which is open, intelligent and adjustable and able to offer and negotiate requested services with the mobile entity. When a roaming mobile entity connects with such a network, the PBM system interacts with the Policy Manager of the mobile client and provides a profile-based service differentiation, access control and roaming management to support mobility, requested security and QoS.

In the other case when no PBM system is available, we propose that the mobile entity connects directly to its home network via a Mobile IP-IPSec tunnel with a variation that the IPSec tunnel endpoints are updated dynamically [Pau, 2005]. This enables the mobile entity to establish an IPSec tunnel once and maintain the same tunnel across handoffs. The authentication is performed via Mobile IP–AAA registration messages and QoS control messages are exchanged inside the tunnel based on the SLA with the mobile user (i.e. profile based).

In the case of requests beyond a SLA and registered class-of service from the mobile entity (i.e. runtime out-of-bound requests), such requests can be exchanged with the home or guest network based on their respective support of PBM system. This exchange of messages can be implemented via standard protocols such as COPS, or XML-based services

where both the mobile entity and service provider can negotiate service parameters. Figure 7 shows a request formatted in web service from user *John* for higher bandwidth to perform a Video on Demand service.

PROOF-OF-CONCEPT IMPLEMENTATION

In order to test the feasibility of our proposed model and architecture, we have designed and implemented a testbed to evaluate different handoff scenarios. The presented testbed analyses vertical and hard handoff i.e. a mobile node cannot receive packets simultaneously on two or more interfaces from multiple heterogeneous networks using a common network layer. We have integrated mobility, security and authentication by layering Mobile-IP, IPSec and AAA protocols to provide seamless handoff [Keshariya and Hunt, 2005] while the profile management is performed using WSDL-based web services.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope
xmlns:mi="http://mi.resources.wsdl.telecom.co.nz/message-id"
xmlns:proc="http://proc.resources.wsdl.telecom.co.nz/processed-by">
<soap:Header>
  <mi:message-id>11d1df5a8b9c095fa:f3bfb4dcd7:-9000</mi:message-id>
  <proc:processed-by>
    <node>
      <time-in-millis>1222047000000</time-in-millis>
      <identity>john.anderson@roaminggold.telecom.co.nz</identity>
    </node>
  </proc:processed-by>
</soap:Header>
<soap:Body>
  <po:bandwidthReuqest Date=" 1253584800000000"
      Xmlns:req="http://mi.resources.wsdl.telecom.co.nz/requests">
      <req:accountName>
        john.anderson@roaminggold.telecom.co.nz          <!– Username–>
      </req:accountName>
      <req:accountNumber>70874523</req:accountNumber>  <!– Account –>
      <req:service>
         <req:servicename>VoDPlatinum</req:servicename>
         <req:timestart-in-mills>
              1253584800000                          <!– 2009-09-22 14:00:00–>
         </reqtimestart-in-mills>
         <req:timefinish-in-millis>
              1253595600000                          <!– 2009-09-22 17:00:00->
         </req:timefinish-in-millis>
      </req:service>
 </soap:Body>
</soap:Envelope>
```

Figure 7: Web service message for out-of bound request

Windows Implementation

The implementation of the proposed architecture in a Windows environment is shown in Figure 8, where the mobile node has currently three interfaces (WiFi, Ethernet and 3G network). The WiFi interface has detected an available WLAN network together with its associated security and status information. The cost attribute is derived from an external profile while the priority is derived from the internal profile.

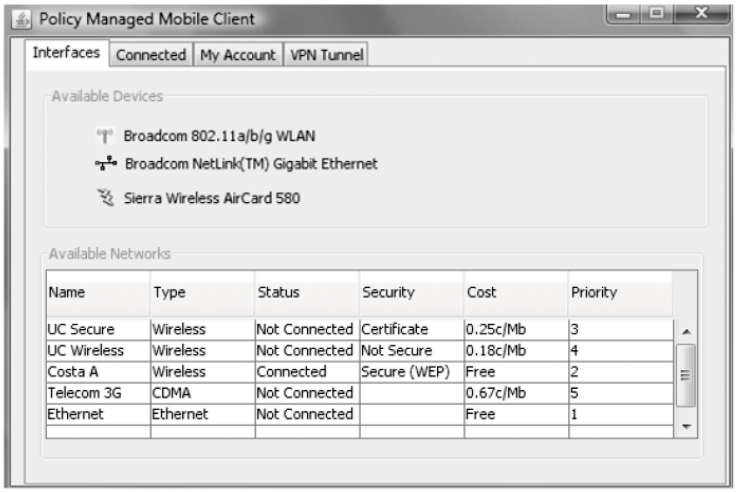

Figure 8: Implementation of Policy Managed Mobile Client

For implementation of the proposed network selection algorithm, a slightly faster method for computing the standard deviation was employed noting that samples are taken once per 100 msec. We have ignored the round-off error, arithmetic overflow and arithmetic underflow to trade-off for the speed for performing calculations. All the experiments were performed on a live network[2].

Figure 9: Signal monitoring based on Internal Profile

Figure 9 shows the monitoring of signal strength of available hotspot areas based on the proposed network selection algorithm. The policy-managed mobile client continually monitors and updates the internal database with available network services and in accordance with the internal profile and performs handoff if a more appropriate access network is available.

TEST RESULTS

We will now present the testbed results to analyse the impact of vertical handoff and overall performance degradation. Throughout our experiments, the mobile device was moved between Home Network (LAN), PBM Managed WLAN (WiFi) and 3G network, and spends the same amount of time in each network. Table 3 presents the average handoff latency over 30 iterations when a mobile entity roams from the LAN to WiFi to 3G network using proposed policy managed mobile client. These iterations were performed three times a day for a period of seven consecutive days.

[2] Courtesy of Telecom NZ

Average Values	*Home Network (LAN) → PBM Managed WLAN (WiFi)*	*PBM Managed WLAN (WiFi) → 3G Network*	*3G Network → Home Network (LAN)*
Time for Registration (sec) When Mobile Node moves to	2.7158	2.8487 – 8.4673	0.1007
Standard Deviation	0.4542	2.3565	0.0521
Packets Dropped (in transactions)	4	7	0

Table 3: Handoff latency when mobile entity roams between networks

Table 4 presents a comparison of registration time when a mobile entity is using the RFC 3344 Mobile IP implementation [Perkins, 2002] as well as our proposed policy managed mobile client, while roaming in networks which are managed with and without PBM systems. Our proposed handoff selection algorithm decreases the handoff latencies with a reduced number of handoffs, hence reducing the total number of dropped packets. We have also observed that the overall improvement in performance is better when the service providing network supports an existing PBM system (Figure 10).

Timing Scales (sec) of Mobile Node while roaming through Foreign network back to Home Network	*Original Delays*	*Avg. Packets Dropped (Ping packets from Goggle)*	*Delays after using scripts*	*Avg. Packets Dropped (Ping packets from Goggle)*
Registration Time (Register to Foreign Agent)	2.766879 3.037013 4.025436	6	0.536383 0.789884 1.442145	2
Deregistration Time (Deregisters with Home Agent after Returning home)	6.328298 8.341493 9.764649	1	2.065042 6.901789 9.292393	0

Table 4: Comparison of registration time with Mobile IP (RFC 3344) and proposed mobile client

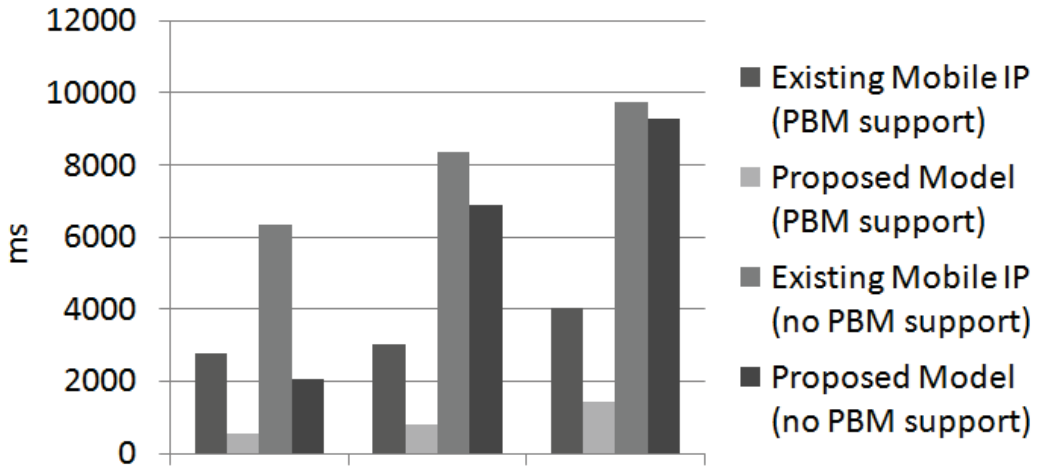

Figure 10: Comparison of dropped packets when proposed handoff selection algorithm is used

Alternative Operating Systems

Although beyond the scope of this paper, implementation of the proposed architecture in operating systems such as Microsoft Windows, Apple Mac OS, Linux, Symbian, iOS, WebOS, Android, and Windows Mobile is very pertinent. Table 5 presents the prospects of our proposed architecture being implemented in these operating systems.

Operating System	Prospects of proposed architecture being implemented/ ported
Microsoft Windows	The proposed architecture was implemented in Windows XP and later tested with Windows Vista and Windows 7.
Linux / Linux-based handheld	Our initial implementation [Hunt and Keshariya, 2005] was based on Dynamics HUT Mobile IP. The mobile client application was later compiled for ARM processor hence it may be possible to run the proposed architecture in other Linux-based handheld devices.
Apple Mac OS X	Based on the available network and wireless tools for Mac OS X and the support for BSD-based command shell, we assume that our application can be rewritten in Objective-C to run on this operating system.
Android	Our proposed mobile client in Windows environment was developed in Java and used Java Native Interface (JNI) to perform network operations. Since Android follows a similar approach with Java-JNI to provide network services, the proposed architecture may be implemented for this platform. Incidentally, some of the work in implementing IEEE 802.21 in the Android platform is well underway in the research community.
iOS	Due to the requirements of Mobile IP protocol to implement IP-in-IP tunnelling and the closed nature of iOS, access to its internal network stack may not be possible,thus affecting the implementation of the proposed architecture. However, iOS support for Virtual Private Networks (which support a similar type of IP-in-IP tunnelling) and availability of various network tools to monitor WiFi and Cellular signals, may derive a possibility to port the native Objective-C application to iOS.
Windows Mobile 7 WebOS	These are relatively recent systems and no information is yet available to determine the feasibility of such an implementation.

Table 5: Implementation of proposed architecture in modern operating systems

CONCLUSION

One of the main challenges in offering always connected services to mobile users is heterogeneity. The diversity in the environments augments the complexity at every stage of the handoff process, from selecting best available network, selecting optimum time to handoff to continuous analysis of dynamic network conditions. As the mobile user wants to be connected at all times with acceptable QoS and security, a number of decisions are required to fully support and to some extent automate a seamless and transparent handoff.

In this paper, we have proposed a model and its architecture of a policy-managed mobile client to support handoff across multiple networks. Our mobile client architecture supports multi-domain authentication and security for different mobility scenarios. The proposed novel network selection algorithm and the Infrastructure parameter help in selecting an optimum time and the best available network for handoff, and to perform a handoff only if required. The performance analysis in Windows environment of the proposed architecture showed the improved overall performance resulting in reducing the number of handoffs and minimising the number of dropped packets, which validates our architectural framework.

REFERENCES

Frodigh, M., et al., *Future-generation wireless networks.* Personal Communications, IEEE, 2001. 8(5): p. 10-17.

Lu, W., *Fourth-generation mobile initiatives and technologies [Guest Editorial].* Communications Magazine, IEEE, 2002. 40(3): p. 104-105.

Perkins, C., *RFC 3344: IP Mobility Support for IPv4.* Network Working Group, 2002.

Strassner, J., *Policy Based Network Management - Solutions for the Next Generation*, R. Adams, Editor. 2004, Morgan Kaufman Publishers. p. 3-16.

Boutaba, R. and Polyrakis, A., *Extending COPS-PR with Meta-Policies for Scalable Management of IP Networks.* Journal of Network and Systems Management, 2002. 10(1): p. 91-106.

He, H. et al, *Web services architecture usage scenarios.* W3C Working Group Note, 2004.

Moffett, J. and Sloman, M., *Policy Conflict Analysis in Distributed System Management.* Journal of Organisational Computing, 1994. 4: p. 1-22.

Feng, F. and Reeves, D, *Explicit proactive handoff with motion prediction for mobile IP*. in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNCt'04)*. 2004.

Stemm, M. and Katz, R., *Vertical handoffs in wireless overlay networks.* Mobile Networks and Applications, 1998. 3(4): p. 335-350.

Tripathi, N. et al, *Adaptive Handoff Algorithms for Cellular Overlay Systems using Fuzzy Logic*, *IEEE 49th Vehicular Technology Conference*. 1999.

Park, H. et al. *Vertical handoff procedure and algorithm between IEEE802. 11 WLAN and CDMA cellular network*. 2002: Springer-Verlag.

Hunt, R. and Keshariya, M, *Proposal for an Automated Algorithm for Optimised Handoff in Integrated Wireless Networks*. *Network and Communication Systems, NCS 2005*. 2005. Krabi. Thailand.

Pau, V., *Development of Secure IPsec Tunnelling in a Mobile IP Architecture.* www.cosc.canterbury.ac.nz/research/RG/i-net_security/papers.htm, 2005.

Keshariya, M. and Hunt, R., *Implementation of an Integrated Secure Mobile Wireless Architecture*. *Network and Communication Systems, NCS 2005*. 2005. Krabi, Thailand.