Over-the-Air Management of Multi-Mode Mobile Hosts using SNMP

T. S. Randhawa  
NewMIC Scientist  
SierraWireless Cluster  
New Media Innovation Center (NewMIC)  
Vancouver, BC, Canada V6B 5K3  
tel: 604.806.5131  
email: tejinder.randhawa@newmic.com

R.H.S. Hardy (Corresponding Author)  
Professor  
School of Engineering Science  
Simon Fraser University  
Burnaby, BC, Canada V5A 1S6  
tel: 604.291.4332  
email: rhardy@sfu.ca

Abstract -- Proliferation of IEEE 802.11 WLANs (Wireless Local Area Networks) is occurring at an unprecedented rate. To realize the benefits of localized yet unlicensed and high-bandwidth WLANs along with highly available but low bit-rate overlay WWANs, the MHs (Mobile Hosts) such as laptops and PDAs are being equipped with multiple wireless NICs (Network Interface Cards). Also growing strongly, as a consequence, is the desire to develop a capability to troubleshoot and manage these devices over-the-air, even when the user is in-transit, so that user’s perception of quality of service and reliance on these multi-mode devices could be improved. However, a key requirement for an MH management system for such multi-mode overlay environments is the ability to handle handoffs between WLANs and WWANs, also known as vertical handoffs.

So far the issue of vertical handoffs has been addressed mostly under the context of TCP (Transmission Control Protocol) based applications. A number of proposals have been made in literature which aim at maintaining TCP connections during vertical handoffs. This is achieved by either deploying mobile-IP or proxy servers, or making alterations to the protocol stack structure. For an MH management service, that may not use TCP as its underlying transport mechanism, such overheads may be deemed unnecessary and expensive. An efficient MH management system is thus needed that could, not only undertake conventional device management tasks, but also maintain access to the MH during vertical handoffs, without imposing unnecessary network or protocol stack overheads.

A novel MH management scheme is proposed herein that addresses the aforementioned requirements in simple yet elegant fashion. The proposed scheme uses SNMP (Simple Network Management Protocol) for managing MHs. An SNMP agent is installed on each MH along with an appropriate MIB (Management Information Base). The mobiles are then managed by a centralized SNMP manager. The handoffs within the WWAN (horizontal handoffs) are left to the native mobility management procedures whereas vertical handoffs i.e. handoffs between WWAN and WLANs are facilitated through SNMP itself. The proposed scheme does not involve mobile IP, external proxies or alterations to the protocol stacks.

Index Terms -- SNMP, mobility management, MH management, vertical handoffs, Mobile IP, GPRS.

I. INTRODUCTION

The subscribers of wide-area wireless data services are growing rapidly. The sheer volume of devices such as laptops and PDAs, currently in use for wireless access, suggests a need for an effective MH management infrastructure so that these devices could be monitored and managed remotely. There is a growing expectation from users as well as service providers that management tasks such as software upgrades, provisioning, trouble-shooting, event management and traffic monitoring of MHs could be accomplished over-the-air, even when the user is in-transit. Given that the wireless technologies are continuously evolving and a global uniform wireless standard is unlikely to materialize in near future, such capability is being perceived as a necessity rather than a ‘nice to have’ feature.

A key requirement for a device or host management system for mobile environments is the ability to track and access the mobile hosts continuously. In WWANs, the mobility management is the responsibility of the underlying network protocols and is performed transparently to the applications. In GPRS (General Packet Radio Service), for example, logical network nodes called GSNs (GPRS Support Nodes) are used for packet routing in the backbone [1]. The GGSN (Gateway GSN) acts as the interface to the public data network and contains the routing information to be used for tunnelling packets to the MH through SGSN (Serving GSN). The SGSN is responsible for location management and delivery of packets. Packets originating from the MH are routed to its destination by SGSN. Packets intended for an MH reach the GGSN associated with its home network. The GGSN determines which SGSN is serving the MH, encapsulates the packet and tunnels it to the SGSN. One can therefore easily envisage an MH management application utilizing the underlying network support for mobility management to achieve continuous access to the MHs. Porting device management applications from fixed to mobile environments should be conceptually feasible, at least from device access perspectives, as long as the mobility is handled transparently by the underlying network. The increasing use of WLANs, in addition to WWANs, for Internet access is, however, changing this premise.

The continuing expansion of coverage in the unlicensed ISM band is encouraging users to equip their MHs with multiple NICs to experience the best coverage combination of overlay WWANs and WLANs. WWAN subscribers are adding WLAN NIC to their laptops and PDAs to take advantage of
this unlicensed yet high bandwidth coverage. The mobility implications here are that once a user detaches itself from the coverage of WWAN and associates itself to a WLAN, its mobility is no longer managed by the mobility management procedures of the WWAN, and thus may become inaccessible to the MH manager. A global mobility management strategy is thus needed so that a multi-mode MH could be accessed anywhere and anytime for trouble-shooting and proactive management purposes.

Numerous internetworking architectures and configurations have been proposed to support vertical handoffs, and maintain accessibility to the mobiles at all times [2][3][5]. The most widely discussed architecture involves Mobile IP [2][5]. The Mobile IP enables a computer to move to a new network without changing its IP address or disrupting communications connections [4]. The Mobile IP architecture introduces two new functional entities called home agent and foreign agent which cooperate to allow a mobile host to move without changing its IP address. Each mobile host is associated with a home network on which a designated host acts as its home agent. When the mobile host is away from home network home agent is responsible for intercepting and forwarding packets destined to it. The GGSN and SGSN of GPRS can be thus be considered as the Mobile IP equivalent of the home agent and foreign agent, respectively.

The support for vertical handoffs in hybrid WLAN/WWAN environments using Mobile IP is achieved by adding Mobile IP’s foreign agent functionality to the WWAN gateways. As an example, in GPRS & IEEE 802.11 based overlay networks, within the GPRS service area the mobility is managed locally. The GGSN is enhanced to act as a Mobile IP foreign agent that enables Mobile IP to keep track of which network the mobile is currently in, as illustrated in Fig. 1. Similar capability can also be achieved by using proxy servers, in place of Mobile IP, as described in [2]. Other methods involve changing the protocol structure to introduce WLAN/WWAN inter-networking [3].

The main drawback of the above proposals is the additional overhead that is introduced in the network architecture as well as the protocol structure. This is primarily due to their aim of keeping TCP connections alive even during vertical handoffs. Alternative schemes are thus needed for MH management applications that may use UDP, in place of TCP, and thus may avoid unnecessary overhead.

Based on the above implications and considerations, we propose herein an SNMP based simple yet elegant method of MH management. The proposed approach uses SNMP not only for managing MHs but also exploits its features, such as asynchronous traps, to facilitate vertical handoffs. The proposed scheme does not involve mobile IP, external proxies or alterations to the protocol stacks.

![Fig. 1. Mobile IPv4 based GPRS and IEEE 802.11 Hybrid Network](image)

Although SNMP is a widely used protocol for managing devices such as network routers and switches, its role in managing wireless MHs has always been questionable due to two main reasons e.g. resource constraints and security concerns. This perception is however changing. The computing and memory power of laptops as well as PDAs is approaching that of desktops. Recent advancements in micro fuel-cell technology are expected to significantly enhance the battery life. Supporting an SNMP agent on a PDA is thus no longer a resource constraint. As far as security issues are concerned, in SNMP version 3, the USM (User based Security Model) is defined, which provides authentication and privacy services for SNMP [6]. The USM is designed to prevent against the threats such as modification of information, masquerade, message stream modification and disclosure that makes SNMP far less susceptible to security breaches. Last but not least, the emerging ad-hoc wireless network configurations involve no central AP (Access Point) or base station. As a result, any participating MH may be required to act as a relay to support communications among other MHs. The MH functionality in these configurations thus approaches that of a router. A widely used and well tested protocol such as SNMP can not be overlooked as a potential candidate for managing MHs in such networks.

The rest of the paper is organized as follows. Section II describes the proposed scheme for over-the-air management of multi-mode MHs. In Section III the main features of the experimental test-bed used to verify the proposed scheme are
highlighted. Finally, Section IV makes some conclusions and, once again highlights the main contributions of this work.

II. SYSTEM MODEL

Consider the system setup of Fig. 2 where an overlay coverage from GPRS WWAN and IEEE 802.11 WLANs is assumed. GPRS coverage is assumed to be always available whereas IEEE 802.11 coverage is expected to have intermittent gaps. Each MH supports an SNMP agent and a MIB. An SNMP trap is also defined which gets generated whenever the IP routing table in the MIB is updated. The SNMP Manager is a stationary entity with a fixed IP address, and is always accessible to an MH. The MHs are dual-mode and are therefore assumed to be equipped with WLAN as well as WWAN NICs.

An MH user may utilize local-coverage high-bandwidth data networks such as IEEE 802.11 whenever available and switch to an overlay service such as a GPRS network with low bandwidth when the coverage of a WLAN is not available. Such transfer of connection, or a Vertical Handoff, is initiated and controlled by a mode detection & switching (MDS) component. The MDS is a simple process that runs on top of the transport layer of the protocol stack at the MH.

The MDS continuously monitors the received signal strength. Once the received signal strength crosses the threshold and stays above it for certain amount of time (dwell time), the handoff is initiated. The dwell timer is started the instant the signal strength of WLAN beacon messages is observed to be higher than the threshold. If the condition stays true until the timer expires the vertical handoff is performed.

The vertical handoff from GPRS to IEEE 802.11 involves three steps. Firstly, the DHCP (Dynamic Host Configuration Protocol) client on the device is invoked to request a routable IP address for the WLAN NIC. The DHCP server returns an available IP address out of the pool of addresses, which is not already allocated to the local network. Secondly, once the IP address is configured properly and it appears in the IP routing table of the MH, the MDS updates the IP routing table. The cost metric corresponding to the newly acquired IP address entry in the routing table is modified to make it the preferred choice for any future data transmission from the device. The routing table update causes an asynchronous SNMP trap, as pointed out earlier. The SNMP trap is intercepted by the SNMP manager. Since the SNMP trap PDU (Packet Data Unit) leaves the MH through the IEEE 802.11 NIC (due to the aforementioned routing table update), the source address in the PDU is the newly acquired IP address of the WLAN NIC. The manager recovers the source IP address and uses it for future communication with the SNMP agent on the MH. Lastly, a GPRS Detach may be invoked by MDS to preserve battery power and avoid unnecessary signaling load to the GPRS network.

The SNMP manager also maintains association of MHs with the dynamic IP addresses allocated to their wireless NICs. As IP addresses of the NICs are expected to frequently change, each MH is assigned a unique ID so that it could be identified irrespective of the IP addresses allocated to its NICs. The MH ID is stored as a MIB variable so that it could be easily queried by the SNMP manager to identify the device. This solves the problem of one device leaving the WLAN, and another device entering that WLAN and (its NIC) being assigned the same IP that the previous device had.

The vertical handoff from IEEE 802.11 to GPRS also follows a similar pattern. When the device moves out of the WLAN, a deterioration in signal strength is detected by the MDS. Again, three main steps are followed. Firstly, the MDS performs a GPRS attach which activates the PDP context. The PDP contexts contain mapping and routing information for packet transmission between MH and GGSN. For each GPRS communication of an MH, a PDP context is created to characterize the session. After the PDP context activation, the MS is known to the GGSN, and communication to external networks is possible. Assuming that dynamic IP addressing scheme is specified in PDP context (the static IP addresses are used mostly for business users), a suitable IP address is allocated to the mobile through ‘Activate PDP Context Accept’ message. Secondly, as the new IP address appears in the routing table, the MDS updates the cost metric to make the GPRS NIC as the preferred one for any future outgoing packets. This automatically generates another SNMP trap that, as described earlier, is used to notify the manager of the vertical handoff and inform it of the new IP address to be used as the destination address for communicating with the SNMP agent on the MH. In case static address-
If an IP address is used in the PDP context, then the IP address of the GPRS NIC stays the same, however the trap is still initiated.

Fig. 3. SNMP based Vertical Handoff Support

III. EXPERIMENTAL TEST BED

An experimental test bed was constructed for the proof-of-concept purposes, similar to the one illustrated in Fig. 2. Compaq’s iPAQs with dual-slots were used as mobile devices. Orinoco’s WaveLAN access cards were used to access IEEE 802.11 whereas GPRS access cards were chosen to be Sierra Wireless’s AirCard 750. The IEEE 802.11 access points were IBM’s Wireless LAN Access Point 500. The RedHat linux servers, with IP forwarding enabled, were used as routers to create multi-hop and multi-subnet network. Each IEEE 802.11 AP was used to create a separate wireless subnet.

The SNMP agent, developed at University of California Davis was deployed on each mobile device, along with a small MIB [7]. A multi-threaded MH manager was developed using jSNMP. The device manager was programmed to periodically monitor the counts of incoming packets and outgoing packets on each NIC of the MH. The viability of the approach was verified by observing that the SNMP manager successfully maintained communication with the SNMP agent on the MH even while the MH traversed multiple WLANs and WWAN, and continued to perform the MH management tasks such as traffic monitoring seamlessly.

IV. CONCLUSIONS

Mobile hosts with multiple wireless NIC are becoming the norm. The multi-mode nature of mobile devices however adds to the complexity of various applications including mobile host management systems. An MH management system is now expected to support management tasks such as over-the-air software upgrades, device provisioning, trouble shooting and monitoring seamlessly even if the mobile host is moving across WLANs and WWANs. Although a number of proposals have been made in recent years to support mobility and vertical handoffs in hybrid WLAN/WWAN environments, most of these proposals either demand additional components in the network infrastructure or alterations to the already deployed protocol structures. We conjecture herein that such overhead may be unnecessary for management applications.

We therefore propose herein a device management infrastructure which addresses the aforementioned requirements in a simple yet effective manner. The proposed system exploits functionality of SNMP in not only performing the conventional MH management tasks but also supporting global mobility management in hybrid WLAN/WWAN environ-
ments. The viability of the approach is verified using an experimental test-bed.

The main contribution of the work is that it highlights capability and potential of SNMP in multi-mode MH management service that has not been explored before.

REFERENCES

[1] GSM Specification 03.60, “General Packet Radio Service (GPRS); Service Description; Stage 2”.


