Journal of Computer Science 2 (5): 410-418, 2006
ISSN 1549-3636

Mobile Agents in Wireless LAN and Cellular Data Networks

R. B. Patel, V. K. Katiyar and Vishal Garg
Department of Computer Engineering, M. M. Engineering College, Mullana-133203, Haryana, India

Abstract: Advancing technology in wireless communication offers users anytime, anywhere access to information and network resources without restricting them to the fixed network infrastructure. Mobile computing represents a shift in the distributed systems paradigm. The potential of decoupled and disconnected operation, location-dependent computation and communication and powerful portable computing devices gives rise to opportunities for new patterns of distributed computation that require a revised view of distributed systems. Mobile environment brings different challenges to users and service providers when compared to fixed, wired networks. Mobility brings uncertainties, as well as opportunities to provide new services and supplementary information to users in the locations where they find themselves. A mobile user is one who, on occasion, disconnects from his/her home network to change location and then reconnects, possibly using a different access technology. A necessary feature of mobility management is the ability to continue to provide system and network services to mobile users seamlessly, regardless of their location and the form of their connection. In general, most application software, operating systems and network infrastructures are intended for more conventional environments and so the mobile user has great difficulty in exploiting the computational infrastructure as fully as he/she might. The Internet Roaming solution for corporate wireless data users integrates mobile networking across private wireless local area networks (WLANs), public WLANs and cellular data networks. In this study we have developed an infrastructure using mobile agent for integrating the Wireless LAN and cellular data called Internet Roaming System (IRS). It is implemented on PMADE mobile agent system developed at IIT Roorkee.

Key words: Wireless LAN, mobile agent, MCMA, SGMA

INTRODUCTION

Wireless local area networks (WLANs) and cellular data networks are complementary technologies. WLANs have several advantages over cellular networks, including higher speed and lower operating and equipment costs. However, their coverage is typically limited to corporate buildings, residences and certain public hotspots. Cellular data networks, on the other hand, provide wide-area coverage but at lower speeds and a much higher cost[1,2]. Naturally, integrating WLAN and cellular data networks to serve users who need both high-speed wireless access as well as anytime anywhere mobile connectivity is the best of both worlds.

Mobile agent technology offers a new computing paradigm in which an autonomous program called mobile agents (MAs) can migrate under its own or host control from one node to another in a heterogeneous network. In other words, the program running at a host can suspend its execution at an arbitrary point, transfer itself to another host (or request the host to transfer it to its next destination) and resume execution from the point of suspension[3]. There are two main areas in which MAs offer considerable advantages, namely: systems and distributed management and information retrieval. Other areas where mobile agents are seen as offering potential advantages, are disconnected computing, also known as wireless or mobile computing, dynamic deployment of code, thin clients or resource-limited devices, personal assistants and mobile agent-based parallel processing[4-6].

Currently, most WLAN-cellular network integration solutions are operator-oriented, the objective being to bundle hotspot public WLAN service with the data service offered by cellular operators[7,8]. In such a setup, the public WLAN service reuses the cellular network's infrastructure and resources, giving users benefits such as a single bill[9]. However, operator oriented solutions are not entirely hassle-free, especially for corporate users. After getting a wireless connection to the Internet via a cellular network or a public WLAN, for example, a corporate user must run a virtual private network (VPN) program to create a secure connection to the corporate intranet. Typically, if the user switches the wireless connection — by moving into or out of a public WLAN's range, for instance — the secure connection breaks, forcing the user to re-launch the VPN program to reconnect. Moreover, operator-oriented integrated solutions only cover public WLANs in hotspots, not private WLANs such as office and residential-telecommuting WLANs (which could

Corresponding Author: R. B. Patel, Department of Computer Engineering, M. M. Engineering College, Mullana-133203, Haryana, India

require different connection and security configurations of the WLAN adaptor on the user's system). Corporate users roaming between these environments need to frequently change their WLAN configurations - a burdensome and error-prone task[10]. Mobile agents can replace VPN programs. In our model agent submitter (AS)[3,11] perform this task and is fully platform/network independent.

Our prototype WLAN-cellular network integration solution, called Internet Roaming System (IRS) lets corporate users create a secure connection using a single sign-on authentication interface, regardless of which wireless network their system is connected to. Once the secure connection is created, the system produces a computing environment that doesn't change, even if the user moves from one wireless network to another. In addition, we designed IRS to use existing technologies as much as possible, including mobile agents[3-5], Mobile IP[12], the IP security protocol (IPsec)[13] and various wireless access methods. IRS is implemented on PMADE mobile agent system developed at IIT Roorkee[3]. We have also done comparison performance of some existing router.

Overview of PMADE: Figure 1 shows the basic block diagram of PMADE. Each node of the network has an Agent Host (AH), which is responsible for accepting and executing incoming autonomous Java agents and an Agent Submitter (AS)[11], which submits the MA on behalf of the user to the AH.

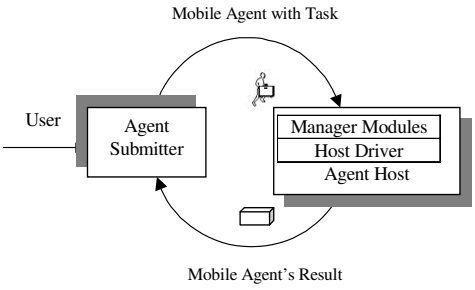

Fig. 1: Block architecture of PMADE

A user, who wants to perform a task, submits the MA designed to perform that task, to the AS on the user system. The AS then tries to establish a connection with the specified AH, where the user already holds an account. If the connection is established, the AS submits the MA to it and then goes offline. The AH examines the nature of the received agent and executes it. The execution of the agent depends on its nature and state. The agent can be transferred from one AH to another whenever required. On completion of execution, the agent submits its results to the AH, which in turn stores the results until the remote AS retrieves them for the user.

The AH is the key component of PMADE. It consists of the manager modules and the Host Driver. The Host Driver lies at the base of the PMADE architecture and the manager modules reside above it. It is the basic utility module responsible for driving the AH by ensuring proper co-ordination between various managers and making them work in tandem. Details of the managers and their functions are provided[14]. PMADE provides weak mobility to its agents and allows one-hop, two-hop and multi-hop agents[15].

System architecture: It is assumed that mobile computing system consists any number of mobile hosts (MHs) connected through one or more base host (BH) (called Mobile Service Stations (MSSs)) also known as servers, over some wireless network like infrared. MH will often be disconnected for prolonged period of time due to the low power of battery or unreachable of signal but they will also frequently reallocate between different BHs at different time. Mobile computing environment no longer requires users to maintain a fixed and universally known position in the network and enables unrestricted mobility of the MHs. There may be any numbers of BHs, which communicate through the existing wireless Ad-hoc network infrastructure. It is suggested that there should be a BH in between Internet and other network for providing mobility to the heterogeneous mobile device among heterogeneous networks.

The IRS handles networking in the context of a corporate intranet, four types of wireless networks (office, residential and public WLANs and a cellular data network) and the Internet (Fig. 2). The main objective is to provide secure IP mobility functions for the user's system and to keep that connection alive as the user moves among different wireless networks. Although different users may use different types of cellular data networks, Internet roaming only models one type of cellular data networks. This is because a mobile system usually has at most one cellular data modem installed and it does not need to be changed since the cellular network is designed to support roaming across a wide region, which typically satisfies the user's cellular coverage needs. IRS consists of a virtual single account agent (VSAA) deployed on a corporate intranet, a secure mobility gateway agent (SMGA) deployed between the public Internet and the corporate intranet and the mobile clients managing agent (MCMA) installed on the user systems. We designed the system's architecture to provide an independent add on solution for the corporate intranet. That is, installing the system only involves the deployment of an SMGA and a VSAA at proper locations on the intranet and installation of the MCMA on the mobile system of every user who needs secure mobile networking functions. The MCMA is a suitably configured for the mobile laptop or PDA that users can

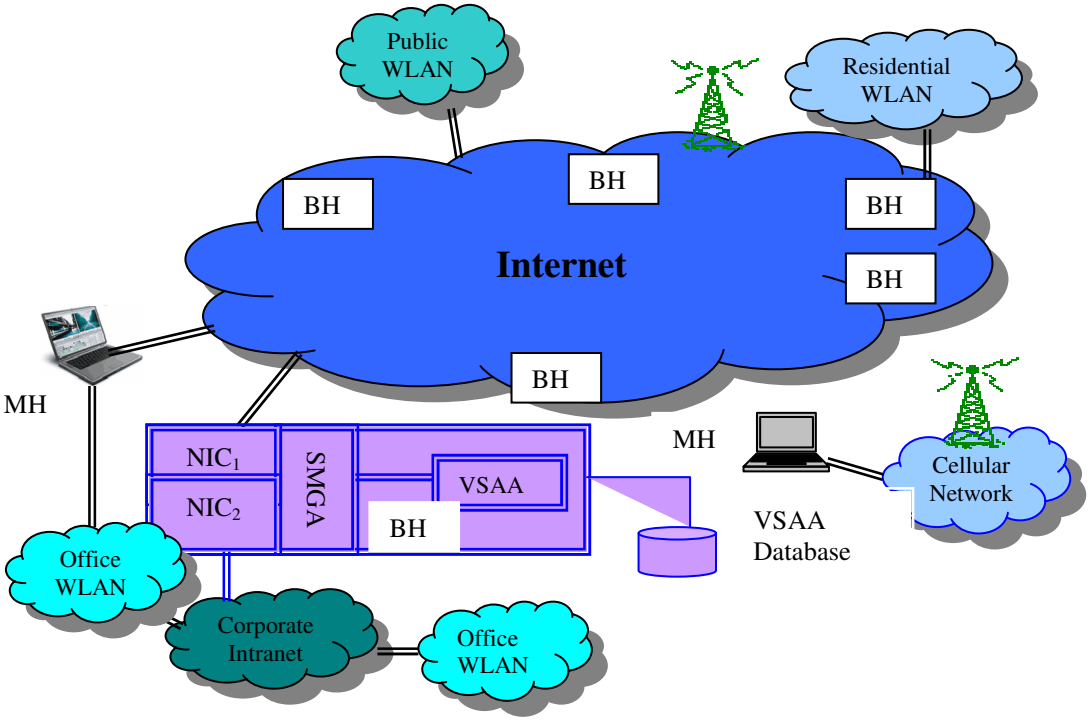

Fig. 2: Internet roaming system architecture

install. No existing networking equipment or services need to be modified.

Virtual single account agent (VSAA): The VSAA provides several functions. It stores every authentication credential used to access wireless networks and the intranet. It also serves as a back-end authentication server for the SMGA and provides an interface for system administrators to manage each user's access rights and authentication credentials. It also provides authentication-credential-updating services to the MCMAs.

The VSAA stores access credentials in a VSAA record, which contains a user's single sign on VSAA certificate, an intranet profile, a cellular profile and several WLAN profiles. Multiple profiles are needed because we assume the user will need to use various networks that can be managed by different entities and that will typically have different configuration parameters. The intranet profile contains the user's authentication credential for accessing the corporate intranet; the cellular profile contains the commands and parameters needed to establish a cellular data connection. A WLAN profile contains configuration parameters, access parameters and an authentication credential. The configuration parameters include the WLAN type (office, public, or residential), the device level authentication method (open or shared-key), the wired equivalent privacy (WEP) key status (on or off), the WEP key value (fixed or dynamically assigned), the WEP enhancement mode (40 bit, 128 bit, temporary key integrity protocol, or 802.11i), the IP initialization method (DHCP or static IP) and the IP configuration (the IP, DNS server and default router addresses). The authentication credential depends on the access parameters: the access method (WEP, 802.1x, IPsec, or browser-based) and the authentication protocol. If the access method is WEP-based, for example, the credential is the WEP key value.

In all profiles, the authentication credential is encrypted via a key derived from the VSAA certificate. Only random data can be used as authentication credentials and only the random portion of authentication credentials are encrypted. It cannot be directly encrypted because it contains descriptive text; instead, only the public key value in the security certificate and the corresponding private key, which are random sequences, are encrypted. The purpose is to avoid offline dictionary attacks against the VSAA certificate if a user's system containing the VSAA record is lost. The encrypted authentication credentials are random, a hacker can test the attack's success only by trying it online, which is time consuming and can easily trigger an alarm.

A system administrator establishes a VSAA record based on the user's job requirement. If a user is not authorized to access a cellular network, for example, no cellular network profile is configured in the VSAA record. In addition, all authentication credentials, including certificate, are generated using random numbers when the system administrator creates them. The user does not need to remember or know them.

The VSAA concept is the single sign-on function's foundation and the MCMA and VSAA jointly support

it. Initially, the MCMA has an empty VSAA record and the user gets a VSAA certificate. For the first-time connection, the user must connect to the wired office intranet and launch the MCMA with the authentication certificate. The MCMA then downloads the user's VSAA record from the VSAA database. After this, whenever the user successfully connects to the corporate intranet, the MCMA contacts the VSAA to download the updated portion of the VSAA record.

Secure mobility gateway agent (SMGA): The SMGA is a special IPsec gateway deployed between the public Internet and the corporate intranet. It authenticates a user's system with the VSAA's help, tracks the system's location with the MCMA's help and relays IP packets between the Mobile device and other IP nodes. The IP packets transmitted between the SMGA and the Mobile device's current location are encrypted and encapsulated.

The SMGA running server has two-network interface cards- NIC_1 and NIC_2: NIC_1 connected to the Internet and NIC_2 to the intranet. The Internet interface (NIC_1) is a hardened host interface: it accepts/sends only mobile IPsec packets, with a destination/source IP address being the Internet interface's IP address. We have designed a mobile-IPsec packet structure based on existing IPsec and Mobile IP technology. A mobile-IPsec packet is a UDP packet that carries a security association identifier, an encrypted payload and a message integrity code. The encrypted payload can be an IP packet, a Mobile IP care-of-address (COA) registration message, or an Internet key exchange message. The intranet interface (NIC_2) is a router interface that presents a subnet of the corporate intranet and the IP address presented by the MCMA to the mobile device's operating system belongs to this subnet. In the context of Mobile IP, this subnet is the home network, the SMGA is the home agent and the IP address used by the user's system is that system's home address. Like the Internet interface (NIC_1), the intranet interface (NIC_2) accepts/sends mobile-IPsec packets, with a destination/source IP address being that interface's IP address. However, it also sends/accepts regular IP packets whose source/destination IP address is the home address of one of the mobile user system. By using mobile-IPsec packets, a single IP-in-UDP tunnel between an MCMA and the SMGA suffices for both security and mobility.

The SMGA stores security association and location information in memory for every wireless user's system[14]. Every security association contains an encryption key for encrypting and decrypting the payload of mobile-IPsec packets. The location information for a user's system consists of a COA and an SMGA interface with which the user's system is communicating. If the user's system is connected to a residential WLAN, public WLAN, or cellular network, the COA is the IP address assigned to the user's system by that network and the SMGA interface used is the Internet interface (NIC_1). If the user's system is connected to an office WLAN, the COA is the IP address assigned to the user's system by that WLAN and the SMGA interface used is the intranet interface (NIC_2). As the user's system moves, both the COA and the SMGA interface might change. Whenever the SMGA receives a mobile-IPsec packet that carries a valid Mobile IP COA registration message or Internet key exchange message, the location information is updated: the new COA becomes this mobile-IPsec packet's source IP address and the new SMGA interface becomes the interface at which this mobile-IPsec packet arrives.

The SMGA interface determines how the user's system is connected to a residential WLAN, public WLAN, or cellular network), the SMGA performs the home agent's relay function using both interfaces NIC_1 and NIC_2. It de-capsulates and decrypts the mobile-IPsec packets arriving at the Internet interface (NIC_1) and then routes the inner IP packets to their destinations via the intranet interface (NIC_2). It also encrypts and encapsulates regular IP packets arriving at the intranet interface (NIC_2) into mobile-IPsec packets and then sends them to the MCMA on the user's system using the Internet interface (NIC_1). If the user's system is connected to an office WLAN, the SMGA performs the home agent's relay function using only the intranet interface (NIC_2). This means that the mobile-IPsec packets transmitted between the SMGA and the MCMA might not need encryption.

There are two reasons the SMGA uses different methods to relay IP packets the system connected to wireless networks on different sides of the boundary between the public Internet and the corporate intranet.

If a user's system is connected to an office WLAN and if the SMGA processes mobile-IPsec packets using only the Internet interface (NIC_1), the mobile-IPsec packets sent from the system to the SMGA's Internet interface (NIC_1) must cross a corporate firewall, which could block them because it can't know the packets' contents (due to encryption).

Using the intranet interface (NIC_2) to serve a system connected to an office WLAN avoids having to encrypt or decrypt the payload, which improves routing speed.

Mobile client managing agent (MCMA): The MCMA is mainly responsible for creating and maintaining a mobile IPsec tunnel between the user's system and the corporate network over the best available wireless network. It interacts directly with and controls, the available wireless, interfaces and Modems. MCMA functions include:

* identifying the best wireless network available
* making proper configurations to connect to the network

* authenticating the user's system to the network
* obtaining a wireless connection and receiving an IP address from the network
* authenticating the user to the SMGA's interface
* creating a mobile-IPsec tunnel to the SMGA's interface
* Performing handoff between wireless networks if the current wireless network is no longer the best one available to the user and
* providing secure mobile routing for the user's system.

In view of operating system, the user's system always employs a static IP address that belongs to the corporate intranet, as if it were a desktop system sitting in the office. Thus, the Internet Roaming solution can reproduce the office network environment exactly for users wherever they are and all networking applications on their systems can run as usual.

Initially, the MCMA presents a consistent single sign on interface for the user to enter the VSAA certificate to start a secure connection to the intranet. The MCMA then identifies the best wireless network available to the user by instructing the WLAN driver to scan the service set identifier (SSID) and measure the received signal strength indication (RSSI) of nearby WLANs.

Several criteria help to determine which available wireless network is best, it is assumed to a cellular network is often available wherever WLAN coverage is not. The MCMA works in conjunction with the wireless modems. If the MCMA detects no WLAN, or if the WLANs detected have SSIDs that don't match a WLAN profile in the user's VSAA record, the best available wireless network is the cellular network specified in the VSAA record. If the MCMA detects a WLAN with an SSID that matches a WLAN profile in the user's VSAA record and with an RSSI value that is above the stated threshold for a quality WLAN signal, that WLAN is the best available wireless network. Finally, if multiple WLANs fit the above description, Intelligent Agent monitoring status of the administrator's system use various preprogrammed priority rules to pick one. For example, the order could be office WLAN, residential WLAN and then public WLAN, with preference for higher RSSI values if there are multiple choices of the same type. This priority order was based on security, throughput, routing performance and cost. If cost is not a factor, the priority order can be office WLAN, public WLAN and then residential WLAN because public WLANs often have faster back-haul connections to the Internet than residential networks too. If the traffic load of a WLAN access point is known, that information could also be incorporated in the selection rules.

After selecting the wireless network, the MCMA computes a key based on the entered VSAA certificate, decrypts the user's authentication credential for the selected wireless network using that key and follows the access method specified in the wireless profile to authenticate the user to the network. After connecting to the network and receiving an IP address, the MCMA decrypts the user's authentication credential for the intranet, authenticates the user to the SMGA's proper interface and creates a mobile-IPsec tunnel between the MCMA and the interface using the Internet key exchange protocol. After all these steps succeed, the MCMA contacts the VSAA to download the updated VSAA record.

Handoff function: After establishing the tunnel, the MCMA keeps monitoring the available wireless networks by instructing the wireless modems to scan for available networks and measure RSSI periodically. This helps the MCMA to determine whether the current wireless network is still the best available (and thus indicates the need for a handoff operation). A handoff may require switching from one wireless modem to another, or it might only change configuration profiles with the same modem. If the current network is a cellular network, the MCMA searches to see if a WLAN (higher speed, lower cost) is available. If the current wireless network is a WLAN and the RSSI value is below the threshold, the MCMA tries to search for other networks. If no other WLANs exist, the cellular network specified in the VSAA record (if available) is the best available wireless network. If there are other WLANs, the MCMA evaluates all the detected WLANs via their types and RSSI values according to the criteria mentioned earlier. After ensuring the availability of another network that is better than the current network, the MCMA directs a handoff operation to the most suitable network by controlling the modem interface.

If a handoff decision is made, the MCMA decrypts the authentication credential for the new wireless network using the key derived from the VSAA certificate and authenticates the user. After obtaining a new wireless connection and receiving a new IP address from the wireless network, the MCMA reports that address as its COA to the SMGA's interface via a Mobile IP COA registration message. Because they are not tied with the mobile-IPsec tunnel end's IP address, the security associations that have not expired need not be updated after handoff.

Routing function: The MCMA also controls network routing for security and efficiency. If the user's system is connected to a residential WLAN, public WLAN, or cellular network, the outbound routing process follows:

* The operating system directs an IP packet to an IP node communicating with the user's system, i.e., the IP packet is actually sent to the MCMA.
* The MCMA encrypts and encapsulates the IP packet into a mobile-IPsec packet and directs it to

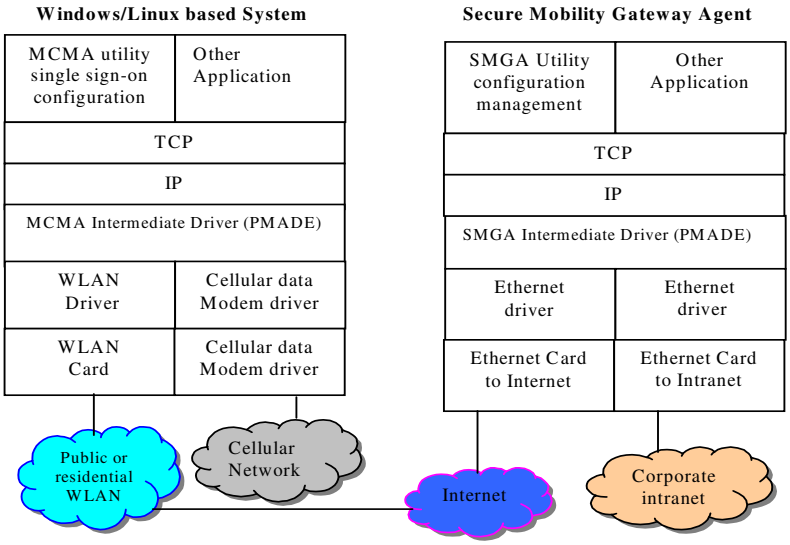

Fig. 3: Architecture of the MCMA on a mobile system and a secure mobility gateway agent (SMGA) located between the corporate intranet and the Internet.

the SMGA's Internet interface, packets sent to the next-hop router on the wireless network and

* The SMGA receives the mobile-IPsec packet from its Internet interface, de-capsulates and decrypts the inner IP packet and then forwards it to the IP node using the intranet interface, packets sent to the next hop router on the corporate intranet.

The inbound routing process, in which the packet's destination IP address is the system's home address, essentially reverses the outbound case. If a network address port translation box is present in the current wireless network, the mobile-IPsec tunnel is not affected due to the use of IP-in-UDP encapsulation. If the user's system is connected to an office WLAN and if encryption is turned off to improve routing speed, the outbound routing process follows:

* The operating system directs an IP packet to an IP node,
* The MCMA receives the packet, encapsulates it into an unencrypted mobile-IPsec packet and then addresses it to the SMGA's intranet interface and
* The SMGA receives the packet from the intranet interface, decapsulates it and forwards the inner IP packet to the IP node using the intranet interface.

Implementation of the system: We have developed a software-based prototype of the IRS for the Windows/Linux operating systems. To maximize its marketability, Internet Roaming must be compatible with Windows/Linux operating systems, which do not offer native mobility support. To achieve this key requirement, we have developed a Windows/Linux based MCMA and SMGA that can jointly support enhanced Mobile IP functions, such as encrypting mobile-IPsec tunnels using the 128- bit advanced encryption[15]. The prototype system enables a Windows/Linux based system to roam seamlessly between WLANs attached to different subnets.

Architecture of the MCMA have an MCMA utility (an application program) and an MCMA intermediate driver (a kernel program, i.e., PMADE) (Fig. 3). The MCMA utility presents a single-sign-on interface for user authentication and can configure Internet Roaming parameters. The MCMA intermediate driver is located between the Windows/Linux operating system and the hardware interface. It provides enhanced Mobile IP functions for the user's system without the Windows/Linux operating system being aware of any mobility and security processing of packets by the intermediate driver. To achieve this, the MCMA intermediate driver is programmed to

* supply Windows/Linux with the home address assigned by the SMGA,
* decapsulate and decrypt inbound mobile-IPsec packets into regular IP packets and pass them to Windows,
* encrypt and encapsulate outbound regular IP packets into mobile IPsec packets and send them to the SMGA and
* monitor the attached subnet, apply for an IP address from the new subnet in the event of a change and register the IP address as the COA with the SMGA.

Because the MCMA hides mobility operations from Windows/Linux, it is compatible with all Windows/Linux based networking programs, including existing VPNs clients. Thus, if a VPN remote access method is already deployed, the MCMA can delegate

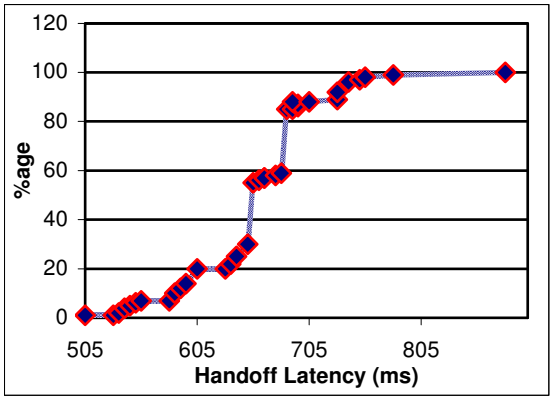

Fig. 4: Cumulative distribution of 802.11bhandoff samples

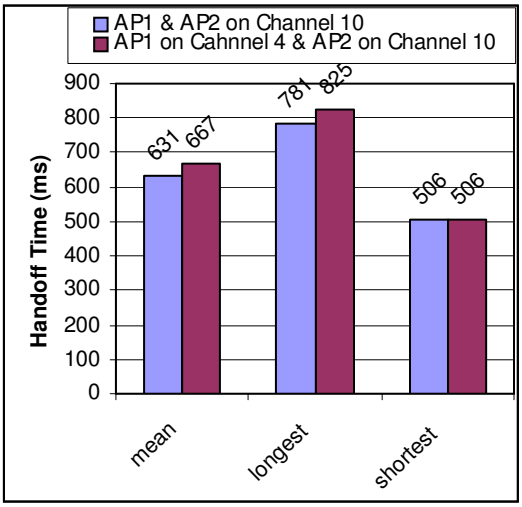

Fig 5:Handoffs for method-2 both AP on same or different channels

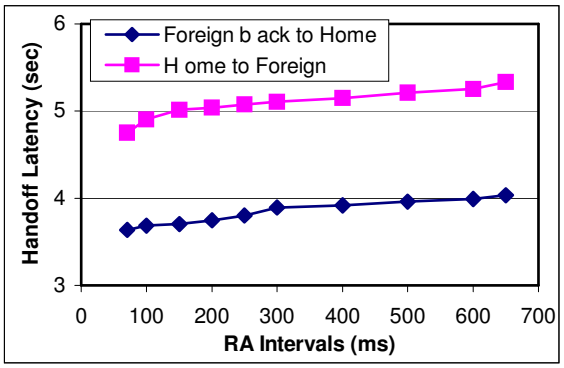

Fig. 6: Handoff times versus RA intervals

security to the VPN when connected to public networks without requiring changes to the existing infrastructure. Similarly, SMGA consists of an SMGA utility and an SMGA intermediate driver (PMADE). A system administrator can use the SMGA utility to configure, monitor and manage users' systems. The SMGA tracks

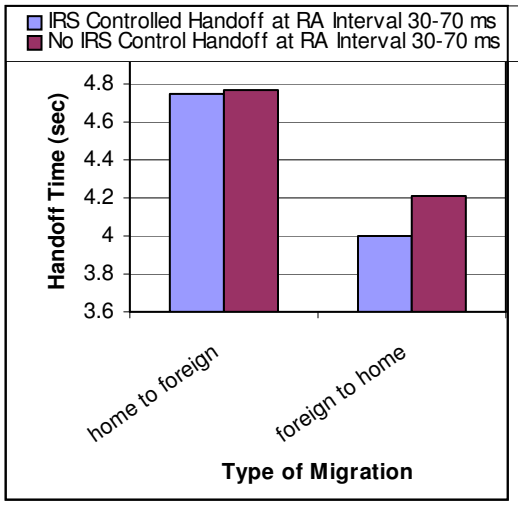

Fig. 7: Handoff including link layer handoff

the location of users' systems and relays IP packets for them.

The MCMA works with a WLAN card and also support the handoff between a WLAN and a cellular data network. In addition, it can communicate with the WLAN driver to access key WLAN parameters such as SSID and RSSI. As a result, we have implemented the wireless network selection criteria and handoff criteria described earlier. In our existing system, all WLANs have to use the same SSID and WEP key. In this scenario, the WLAN driver performs handoffs between these WLANs without awareness of the MCMA intermediate driver. Thus, the MCMA intermediate driver must monitor whether the current WLAN is attached to a new subnet. It does this by periodically sending a unicast address resolution protocol query packet to the default gateway router of the most recently attached subnet. If the number of consecutive address resolution protocol query packets that receive no response exceeds a threshold, the MCMA intermediate driver performs the handoff operations, applying an IP address from the new subnet and registering it as the COA with the SMGA.

Performance study: The performance indices chosen for studying the handoff latency for the IRS are detection time, address configuration time, registration time and packet forwarding time. Detection Time - the time between handoff occurring and the MH (equipped with MCMA) receiving a router advertisement (RA) from the new network access point (AP). Address Configuration Time - the time between the RA and getting a care of address (COA) from the new AP, Registration time - the time from getting a COA to registering the new COA with the home agent (HA) and corresponding hosts and getting the binding acknowledgements and Packet Forwarding Time - is the time from the last binding acknowledgement to the first data packet from the corresponding host.

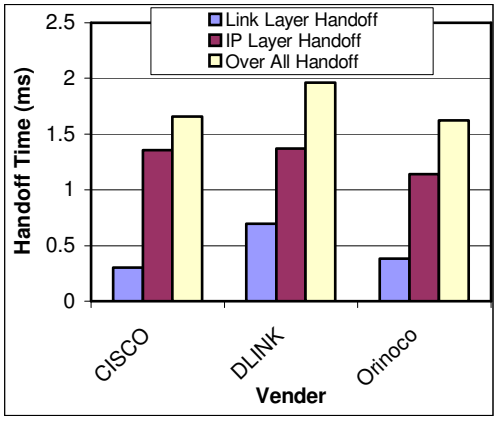

Fig. 8: Handoff delay measurements

We have used two methods to trigger handoff (1) by varying access point power levels (4 Mbps, 10 Mbps, 1000 Mbps) and (2) by alternating MH's service set identifier (SSID) association. We have used three WLANs with three access points (APs) from different vendors (CISCO, DLINK) over a huge Wireless intranet.

We have taken 1000 handoff distribution samples shown in Fig. 4, each case recorded with MH switching simultaneously between two APs, method 2 results in a lower mean handoff value (631 ms compared to 825 ms shown in Fig. 5). MHs keep a list of all recent RAs from all nearby subnets in a cache known as the router advertisement cache (RAC). It also records signal strength, time, etc of the RAC. When the signal strength of the current attachment falls below a predetermined threshold, the MH looks into the RAC and chooses the best subnet for handoff. The MH does not have to wait for a new RA after handoff, so handoff detection time almost zero.

802.11b handoff deals with all 3 phases - detection, search and execution, search phase was the most significant contributor to the handoff latency. The type of wireless card firmware can have a large impact. Our measured handoff is generally longer than reported in other literature. We measure the entire time it takes for actual Ethernet level bridging to successfully resume after re-association with a new (or previous) AP.

We experimentally trigger handoff events and measure the time period during which connectivity was lost shown in Fig. 6. We found that real-world 802.11b handoffs were typically completed in less than 700 ms. The IP level disruption due to 802.11b and IRS controlled handoff together was significantly higher around 4.75 and 3.998 sec. But handoff time for IP level disruption due to 802.11b is higher in comparison to IRS controlled (Fig. 7). Tuning the RA intervals from 30-70ms (the default) to 500-700ms not significantly degrade these handoff times. Short RA intervals may, in practice, not be worth the transmission overhead as shown in Fig. 6. Default IRS controlled handoff is highly disruptive to real-time and interactive applications during handoff events, even if the underlying link layer handoff was instantaneous. How simple implementation bugs can cause substantial increases in the handoff latencies, regardless of the actual IRS system itself.

Figure 8 shows some measurements for the handoff speeds of different WLAN cards. The link layer handoff delay is the difference between the time when the MCMA intermediate driver captures a connect indication event cast by the underlying WLAN driver and the time when the MCMA intermediate driver captures a disconnect indication event. The IP layer handoff delay is the difference between the time when the MCMA intermediate driver captures the connect indication event and the time when the MCMA intermediate driver receives the Mobile IP COA registration acknowledge message from the SMGA, which indicates that the mobile-IPsec tunnel now points to the new COA. Every value is an average of about 1000 measurements of controlled handoff in the same WLAN and wired network environment when channel speed is 1000 Mbps.

Related works: Several commercial products for enterprise-oriented WLAN-cellular network integration exist, such as Ecutel[16], NetMotion Wireless[17] and IP unplugged[18]. Although detailed technical information about these products is not available, we can summarize the major differences between them and Internet Roaming. In these products, the network component equivalent to Internet Roaming's SMGA always uses its Internet interface as an end of the encrypted IP tunnel connected to a mobile system, regardless of which wireless network the mobile system is connected to. With this design, mobile users risk loss of connection if they are connected to an office WLAN inside the corporate intranet. In this case, because the mobile system's COA is with in the corporate intranet and the IP address of the SMGA equivalent component's Internet interface is on the public Internet, the encrypted IP tunnel must cross a corporate firewall. If the firewall does not allow pass through of encrypted IP packets that are unknown to it, the encrypted IP tunnel is blocked and the mobile system will lose the connection. The SMGA addresses this problem, as described earlier. In these products, the client side components equivalent to the MCMA are all software-based and designed for various Windows operating systems. Some of them use WinSock-based mobility management, which could render them incompatible with future Windows releases if WinSock functions are revised.

Others use an intermediate driver to handle security and mobility management, but they need a user space program to pass configuration parameters to the intermediate driver and must start the secure mobile networking functionality manually whenever the system is rebooted. This is inconvenient for laptop users who often want the secure connection to be kept alive after they close the laptop in one location and open it in a new one. Our MCMA solves this problem

because the MCMA intermediate driver, i.e., PMADE can instantly restore the previous secure connection as soon as it is loaded into the kernel when the operating system is rebooting. Thus, the MCMA can always maintain a static office network environment for laptop users as they open and close systems in different locations.

CONCLUSION AND FUTURE RESEARCH

In this study we have developed an infrastructure using mobile agent for integrating the Wireless LAN and cellular data called IRS. We have a software implementation of the SMGA, however and we can implement the VSAA with existing know-how. The MCMA provides a subset of the features and we expect to add the missing functionality as soon as a majority of WLAN interface vendors release drivers that conform to recently published Windows WLAN specifications. The preferred implementation for cellular-WLAN integration requires the availability of suitable dual-interface cellular-WLAN cards with well-specified Windows programming interfaces and drivers.

We are also in the process of hardware based system design in which the iCard can provide the convenience of secure mobile networking for a variety of mobile devices whose operating systems might not provide sufficient support for implementing a software-based MCMA. Our hardware prototype has a small form factor; it looks like an Ethernet card to the mobile system and it uses a wireless modem to provide secure roaming. The hardware prototype is still in the testing stage. Using existing WLAN cards, we can implement roaming across different WLANs. Cellular-WLAN integration will require the availability of a dual cellular-WLAN card in a form factor with well specified Linux driver support for switching between networks.

Our further research is truly in step with Cisco's stated direction that more and more intelligence can be absorbed by and more efficiently delivered through the network infrastructure itself. Following three stages are proposed to conduct future research.

Adapt PMADE infrastructure to Wide Area Networking environment using Cisco's networking equipment. Such an environment can simulate unreliable, bandwidth limited network. Develop and characterize mobile agent applications based on this environment.

Develop mobile agent security features for applications developed in 1st stage. Analyze the way Cisco's technology uses networking infrastructure to satisfy application's need for real-time visibility, security and optimized delivery. Propose how Cisco technology can be leveraged to satisfy similar mobile agent application's routing and security needs.

Work with Cisco to develop prototype/simulated-models for integrating mobile agent application needs such as routing and security into networking infrastructure.

REFERENCES

1. Taylor, M., M. Banan and W. Waung, 1997. Internetwork Mobility: The CDPD Approach. Prentice Hall.
2. Holma, H. *et al*., 2002. WCDMA for UMTS. John Wiley and Sons.
3. Patel, R.B., 2004. Design and implementation of a secure mobile agent platform for distributed computing. Ph.D. Thesis, Department of Electronics and Computer Engineering, IIT Roorkee, India.
4. Tripathi, A.R., T. Ahmed and N.M. Karnik, 2001. Experiences and future challenges in mobile agents programming. Microprocessors and Microsystems, 25: 121-129.
5. Pitoura, E. and G. Samaras, 2001. Locating objects in mobile computing. IEEE Trans. Knowledge and Data Engineering, 13: 571-592.
6. Picco, G.P., 2001. Mobile Agents: An Introduction. Microprocessors and Microsystems, 25: 65-74.
7. Feasibility Study on 3GPP System to WLAN Interworking, tech. report 3GPP TR 22.934 v1.2.0, May 2002; www.3gpp.org.
8. Ala-Laurila, J., J. Mikkonen and J. Rinnemaa, 2001. Wireless LAN access network architecture for mobile operators. IEEE Comm., 39: 82-89.
9. Bostrom, T., T. Goldbeck-Lowe and R. Keller, 2002. Ericsson mobile operator WLAN Solution. www.ericsson.com/ about/publications/review/2002_01/files/2002014.pdf.
10. Lucky, R., 2002.Cannot Connect. IEEE Spectrum, 39: 112.
11. Patel, R.B. and K. Garg, 2004. A new paradigm for mobile agent computing. WSEAS Trans. on Computers, 3: 57-64.
12. Perkins, C., 2002. IP Mobility Support. IETF RFC 2002, 1996, www.ietf.org/rfc/rfc2002.txt.
13. Kent, S. and R. Atkinson, 1998. Security architecture for the internet protocol. IETF RFC 2401, www.ietf.org/
14. Patel, R.B., 2005. Mobile agents location management in global network. Proc. Natl. Conf. on Frontiers in Applied and Computational Mathematics (FACM 2005), Thapar Institute of Engineering and Technology- Patiala, India, Mar. 4-5, pp:148-165.
15. Patel, R.B. and K. Garg, 2003. Providing security and robustness to mobile agents on open networks. Proc. 6th Intl. Conf. Business Information Systems (BIS 2003), Colorado, Spring, USA, Jun. 4-6, pp: 66-74.
16. Mobile VPN Benefits, Ecutel Systems Inc., May 2003, http://www.ecutel.com/solutions/
17. Renfroe, D., 2005. Network Computing. CMP, United Business Media, April, www.nwc.com
18. James, D.S., 1997. Mobile IP-The Internet Unplugged. Prentice-Hall, Inc. Upper Saddle River, NJ, USA.