Wireless data networks present a more constraint communication environment compared to the wired networks. Because of fundamental limitations of power and available spectrum, wireless data networks tend to have less bandwidth, more latency, less connection stability and less predictable availability. Wireless access to Internet services will become typical, rather than the exception as it is today. Such a vision presents greater demands on mobile networks and so things are changing at a rapid rate in this field towards advancement. The growing needs of users to
incorporate multimedia information in hand held devices makes the things more complicated to handle large amounts of data on optimized networks and all the more it makes the environment more prone to external threats in various manners. This paper presents an analysis of the model of Ad Hoc networks design. It also includes a survey of some common security threats to which Ad Hoc networks are exposed to as well as some proposed solutions to deal with such threats. Thus Ad Hoc networks present a situation where not only things have to be made easy for the end user but on the contrary there has to be some tough time for the professional hackers.

Introduction
The development of commodity-based palmtop devices with built-in high-speed packet radio access to the Internet will have a major impact on the way we communicate. Large numbers of mobile users equipped with wireless IP-enabled communicators will have access to a wide array of Web-based mobile multimedia services. Future wireless network infrastructure will have to support a wide variety of users, applications, and access needs. High-speed access can be achieved by using smaller and smaller cell sizes, resulting in coverage areas with a larger number of base stations. One can imagine a scenario where each person’s office has its own access point offering tens to hundreds of megabits per second of wireless access in an Ad Hoc network environment. These types of Pico cellular environments call for simple, low-cost wireless infrastructure that ultimately must compete with wireline LAN service quality, costs, security, and plug-and-play scalability. Mobile users will expect the same level of service quality as wireline users. That will translate to high-speed access with seamless mobility, which we define as the ability of the network to support fast handoff between base stations with low delay and minimum or zero packet loss. As base station density increases, however, so will handoff rates. This places significant demands on future Ad Hoc network architecture, protocols, and services to support seamless mobility. It is believed that support for seamless mobility will be needed in order to provide good service quality to mobile users, particularly in Pico cellular environments where the rate of handoff and associated signaling load grows rapidly. Network support for seamless mobility was not a primary design consideration when Mobile IP was first defined in the early ’90s. More recently the Mobile IP Working Group has been addressing this issue. With frequent handoff micromobility protocols have been proposed [3–6] to handle local movement of mobile hosts without interaction with the Mobile-IP-enabled Internet. This has the benefit of reducing delay and packet loss during handoff, and eliminating registration between mobile hosts and distant Home Agents (HA) when mobile hosts remain inside their local coverage areas. Eliminating registration in this manner reduces the
signaling load experienced by the core network in support of mobility. Reducing signaling in this manner is necessary for the wireless Internet to scale to support very large volumes of wireless subscribers. As the number of mobile subscribers grows, so does the need to provide efficient location tracking in support of idle users and paging in support of active communications. In order to achieve scalable location management, the wireless Internet needs to handle the location tracking of active and idle mobile hosts independently. Support for passive connectivity balances a number of important design considerations. For example, only keeping the approximate location information of idle users requires significantly less signaling, and thus reduces the load over the air interface and core network. Reducing signaling over the air interfaces also has the benefit of preserving the power reserves of mobile hosts.

Network Analysis
Ad hoc network inherits cellular principles for mobility management such as passive connectivity, paging, and fast handoff control, but implements them around the IP paradigm. Cellular IP access networks require minimal configuration (e.g., similar to switched Ethernet LANs), thereby easing the deployment and management of wireless access networks. An important concept in Cellular IP design is simplicity and minimal use of explicit signaling, enabling low-cost implementation of the protocol. In what follows, I present an overview of cellular IP access Ad Hoc networks and discuss support for routing, handoff, and security in these networks.

The Network Model
The universal component of Ad Hoc networks is the base station which serves as a wireless access point and router of IP packets while performing all mobility-related functions. Base stations are built on a regular IP forwarding engine with the exception that IP routing is replaced by Cellular IP routing and location management. Cellular IP access Ad Hoc networks are connected to the Internet via gateway routers. Mobile hosts attached to an access network use the IP address of the gateway as their Mobile IP care-of address. Figure 1 illustrates the path taken by packets addressed to a mobile host. Assuming Mobile IPv4 [2] and no route optimization, packets are first routed to the host’s HA and then tunneled to the gateway.
Figure 1: Ad Hoc IP Access Network Design

The gateway detunnels packets and forwards them toward a base station. Inside an Ad Hoc network, mobile hosts are identified by their home address, and data packets are routed without tunneling or address conversion. The Cellular IP routing protocol ensures that packets are delivered to the host's actual location. Packets transmitted by mobile hosts are first routed toward the gateway and from there on to the Internet. In Ad Hoc networks, location management and
handoff support are integrated with routing. To minimize control messaging, regular data packets transmitted by mobile hosts are used to refresh host location information. Uplink packets are routed from a mobile host to the gateway on a hop-by-hop basis. The path taken by these packets is cached by all intermediate base stations. To route downlink packets addressed to a mobile host, the path used by recently transmitted packets from the mobile host is reversed. When the mobile host has no data to transmit, it sends small, special IP packets toward the gateway to maintain its downlink routing state. Following the principle of passive connectivity, mobile hosts that have not received packets for some period of time allow their downlink routes to be cleared from the cache as dictated by a soft state timer. Paging is used to route packets to idle mobile hosts in a Cellular IP access Ad hoc network.

**Routing**

The Cellular IP gateway periodically broadcasts a beacon packet that is flooded in the access Ad Hoc network. Base stations record the neighbor they last received this beacon from and use it to route packets toward the gateway. All packets transmitted by mobile hosts, regardless of their destination address, are routed toward the gateway using these routes. As these packets pass each node en route to the gateway, their route information is recorded as follows. Each base station maintains a routing cache. When a data packet originated by a mobile host enters a base station, the local routing cache stores the IP address of the source mobile host and the neighbor from which the packet entered the node. In the scenario illustrated in Fig. 1, data packets are transmitted by a mobile host with source IP address X. In the routing cache of BS2 this is indicated by a mapping (X, BS3). This soft-state mapping remains valid for a system-specific time called route-timeout. Data packets are used to maintain and refresh mappings. As long as mobile host X regularly sends data packets, base stations along the path between the mobile’s actual point of attachment and the gateway will maintain valid routing cache mappings, forming a soft-state path between the mobile host and gateway node. Packets addressed to mobile host X are routed on a hop-by-hop basis using this established routing cache. A mobile host may sometimes wish to maintain its routing cache mappings even though it is not regularly transmitting data packets. A typical example of this is when a mobile host receives a UDP stream of packets on the downlink but has no data to transmit on the uplink. To keep its routing cache mappings valid, the mobile host transmits route-update packets on the uplink at regular intervals called route-update time. These packets are special ICMP packets addressed to the gateway. Route-update packets update routing cache mappings as is the case with normal data packets. However, route-update messages do not leave the Ad Hoc network.
Handoff

Cellular IP for Ad Hoc networks supports two types of handoff scheme. Cellular IP hard handoff is based on a simple approach that trades off some packet loss for minimizing handoff signaling rather than trying to guarantee zero packet loss. Cellular IP semisoft handoff exploits the notion that some mobile hosts can simultaneously receive packets from the new and old base stations during handoff. Semisoft handoff minimizes packet loss, providing improved TCP and UDP performance over hard handoff.

**Hard Handoff** — Mobile hosts listen to beacons transmitted by base stations and initiate handoff based on signal strength measurements. To perform a handoff, a mobile host tunes its radio to a new base station and sends a route-update packet. The route-update message creates routing cache mappings en route to the gateway configuring the downlink route cache to point toward the new base station. Handoff latency is the time that elapses between handoff initiation and the arrival of the first packet along the new route. In the case of hard handoff this is equal to the round-trip time between the mobile host and the crossover base station as illustrated in Fig. 2. We define the crossover base station as the common branch node between the old and new base stations, an example of which is illustrated in the figure. In the worst case the crossover point is the gateway. During this interval, downlink packets may be lost. Mappings associated with the old base station are not cleared when handoff is initiated. Rather, mappings between the crossover node and the old base station timeout and are removed. No packets are transmitted along the old path once the route-update message has created a new mapping at the crossover base station that points toward the new base station. Although packets may get lost during a hard handoff, the time taken to redirect packets to the new point of attachment is shorter than that in Mobile IP. This is due to the fact that only a local node has to be notified rather than a possibly distant HA in the case of Mobile IP. There are several ways to reduce packet loss during handoff. One approach relies on interaction between the old and new base stations [5] during handoff. In this case the new base station notifies the old base station of the pending handoff. Packets that arrive at the old base station after notification of handoff are forwarded to the new base station and onto the mobile host. In contrast, packets that arrive at the old base station before notification is complete will be lost. If the notification time (i.e., the round-trip time between the new and old base stations) is not smaller than handoff duration (i.e., the round-trip time between the new and crossover base stations), this approach does not significantly improve handoff. An additional cost of these schemes is that communications, signaling, and information state exchange are required between base stations for this approach to work. To preserve the simplicity of hard handoff, Cellular IP employs a different approach to counter the problem of packet loss.
Semisoft Handoff — After hard handoff, the path to the old base station remains in place until the soft-state cache mappings time out. We leverage this feature to support a new handoff service called semisoft handoff that improves handoff performance while maintaining the lightweight nature of the base Cellular IP protocol in Ad Hoc networks. Semisoft handoff calls for one temporary state variable to be added to the protocol running in the mobile hosts and base stations. Semi-soft handoff scales well for large numbers of mobile hosts and frequent handoff, and comprises two architectural components. First, in order to reduce handoff latency, the routing cache mappings associated with the new base station must be created before the actual handoff takes place. Before a mobile host hands off to a new access point, it sends a *semisoft packet* to the new base station and immediately returns to listening to the old base station.
station. The purpose of the semisoft packet is to establish new routing cache mappings between the crossover and new base stations. During this route establishment phase the mobile host is still connected to the old base station. After a semisoft delay, the mobile host performs a regular handoff. The semisoft delay can be an arbitrary value that is proportional to the mobile-to gateway round-trip delay. This delay ensures that by the time the mobile host finally tunes its radio to the new base station, its downlink packets are being delivered through both the old and new base stations. We observe that downlink packets consume twice the amount of resources during this period. However, this period represents a short duration when one considers the complete semisoft handoff process. While the semisoft packet ensures that mobile hosts continue to receive packets immediately after handoff, it does not, however, ensure smooth handoff between base stations. Depending on the network topology and traffic conditions, the time to transmit packets from the crossover point to the old and new base stations may differ, and the packet streams transmitted through the two base stations are typically unsynchronized. If the new base station is behind the old one, the mobile host will receive duplicate packets, which does not disrupt many applications. For example, TCP will not be forced into slow start due to the arrival of duplicate acknowledgments. If the new base station is ahead, packets will be missing from the stream received at the mobile host. The second architectural component of semisoft handoff resolves this issue of the new base station getting ahead. The solution to this problem is based on the observation that perfect synchronization of packet streams is unnecessary. This condition can be eliminated by temporarily introducing a constant delay along the new path between the crossover and new base stations using a simple delay device mechanism. The device needs to provide sufficient delay to compensate, with high probability, for the time difference between the two streams traveling on the old and new paths. Optimally, the device delay should be located at the crossover base station. The crossover base station is aware that a semisoft handoff is in progress from the fact that a semisoft packet arrives from a mobile host that has mapping to another interface. Mappings created at crossover points by the reception of semisoft packets include a flag to indicate that downlink packets must pass through a delay device before being forwarded for transmission along the new path. After handoff is complete, the mobile host sends a data or route-update packet along the new path. These packets have the impact of clearing the flag causing all packets in the delay device to be forwarded to the mobile host. Base stations only need a small pool of delay buffers to resolve this issue. Packets that cannot sustain additional delay can be forwarded without passing through the delay device. This differentiation can be made on a per-packet basis, using, say, differentiated service or transport (e.g., TCP, UDP, or RTP) codepoints.

Sources of Security Concerns
Securing information from unauthorized access is a major problem for any network. Thus Security is made up of a suite of multiple technologies that solve various authentication, information integrity and identification problems. Security is even a greater problem for Ad Hoc networks, since radio signals travel through open atmosphere where they can be intercepted by individuals who are constantly on move and therefore difficult to track down. Mobile systems are open to a number of security problems that do not exist in stationary counterparts. In a fixed network, the prefix of a subnet is usually configured manually and the location of the prefix is communicated between routers that either have some form of inherent trust model or use a secure protocol. This makes it hard to impersonate someone. Mobile hosts on the other hand must update their location while moving. These location messages make impersonation possible unless properly secured. Ad Hoc networks compound these security problems because packets can be easily snooped over the air interface. Many local exchanges carriers use microwave communications for their inter-LATA calls. Since the frequencies used by carriers is a public information, it is not at all difficult for an intruder to intercept both voice and data transmissions. Some of the major security leaks are:

- **Unauthorized Access to Network Resources via Wireless Hardware**
  It is not uncommon for individuals intent on industrial espionage to scoop up vast quantities of information by placing small scanners at appropriate locations and searching with very powerful algorithms. Important network resources are thus exposed to critically unsafe environments.

- **Eavesdropping on the Wireless Signaling**
  Eavesdropping is a passive form of information theft. An eavesdropping attack occurs when an external element manages to listen in on traffic exchanged between a mobile node and its home agent. For this to happen an attacker needs access to the traffic, this can occur in the following ways. An attacker can get physical access to the network socket and connect a host to the network. It is also possible that a foreign element is close enough to Ad Hoc network to be able to receive packets that are transmitted via radio signals.

**Proposed Design for Security in Ad Hoc Networks and Applications**

There are several ways that can be followed in designing for security of Ad Hoc networks and applications in the real world. Some includes Physical security, Applications and System assisted security, the Encryption process, Firewalls and many others. But I would suggest the following three security features that guard against the above major security concerns in a very effective manner:

- **Fluctuating Frequency**: the technique used for transmitting and receiving data wirelessly.
The Security ID Function.
- Authorization Tables.

It should be understood that these aspects perform over and above, and in concert with, network access security provisions such as username/password protection typically already in effect.

**Security Characteristics of Fluctuating Frequency**

One of the key reasons fluctuating frequency should be used is because of its inherent security qualities. In fact, Fluctuating frequency was first used by the military in order to ensure secure communications. Continuously changing Frequency is difficult to detect and decode because the signal hops from frequency to frequency in a random, repetitive sequence. For successful communications to take place, the transmitter and the receiver must be synchronized and using the same sequence. Ideally an Ad Hoc network should employ fifteen different sequences. Further complicating the task of decoding this signaling is the very short duration a transmitter stays at a given frequency and the time taken by the transmitter to hop to the next frequency. The customer cannot vary these settings.
The Security ID Function

The Security ID is a unique, 20 character alphanumeric string defined and configured by the user. It must be identically configured in every radio intended to communicate with others in the same network. Once configured, the Security ID is reduced to 20 bits by a proprietary, confidential algorithm. It is merged with the radio MAC address (a 12 character field unique to every radio), scrambled and stored using another proprietary, confidential algorithm. It is not possible to access the Security ID either directly from the radio card or over the air. On the radio card the 20-bit Security ID, generated by a confidential, proprietary algorithm, is scrambled with the MAC address of the card. The scrambled data are stored using a confidential memory-mapping scheme with the radio’s EEPROM. To determine the Security ID over the Air is even more challenging. The steps required to pick the Security ID from a broadcast would
be:
• To determine and follow the fluctuating frequency pattern
• To demodulate the bit stream
• To unencode the bit stream
• To determine which of the 20 bits in the 1500 byte packet constitute the Security ID
• To reverse engineer the algorithm which originally reduced the 20 character string to a 20 bit Security ID

There are almost 17 million unique Security IDs are possible (16 domains times the 1,048,576 combinations possible with a 20 bit code). So while it is conceivable that someone could attempt a brute force to break-in a network, the time to be required to do so would exceed 2 years.

Authorization Tables Further Enhances the Security
To further ensure the Ad Hoc network security, a network administrator can provide authorization tables for legal MAC addresses. With proper auditing of a network, one can maintain those tables to ensure that only authorized users are allowed on the network. In addition, if an unauthorized client attempts to gain access to the network, this event will be trapped and reported to administrator.

Enabling Secure Coexisting Wireless Networks
The ability to assign discrete Security IDs is particularly useful in environments where multiple, highly secure wireless networks must coexist in a common geographic area and yet be totally independent of one another. This is easily accomplished by using Domain 1 exclusively for one group of users who share a common Security ID and Domain 2 for a second group of users sharing a common Security ID. Given this configuration, at no time could a Domain 1 user ever gain access to the Domain 2 network and vice versa. Assume that Company 1, on the upper floor of a two-story building, has Security ID enabled and that Company 2, located on the bottom floor of the same building, is using a network with a different Security ID. Even if both companies shared the same Domain, users from one company could not access the network of the other company because of their differing Security IDs.
Security in Action: The Pacific Stock Exchange
The above discussed security features for Ad Hoc networks are considered so secure that they have been used by many of the world’s stock exchanges to transmit highly confidential trading information. Because wireless networks speed transactions, thereby increasing revenues, many stock exchanges offer wireless services to the securities firms comprising the exchange. On a typical exchange, over twenty companies share the same, densely populated trading floor. Security concerns are paramount, to guard against outside eavesdropping as well as improper information flow among member companies on the exchange. The Pacific Stock Exchange, the world’s third busiest, has implemented a wireless network. The network includes twelve network Access Points spread throughout the trading floor and attached to the exchange’s Ethernet LAN. There are six sub-networks, each with two access points attached to a Cabletron SEHI-22 hub connected to a Cisco 4700 router that directs traffic to the appropriate trading company. It is difficult to imagine a more exacting, less forgiving environment in which to test the security features of the discussed network to their limits than the Pacific Stock Exchange

![Secure Wireless LAN](1)

Figure 4: Secure Wireless LAN
Although physically close enough to attach to the lower network, unique security IDs prevent unauthorized access
When Additional Security May be Required

The security features proposed above were with the idea of vast majority of users and applications in mind. For those situations where there is concern that advanced and persistent methods may be used to break LAN security, additional security measures may be desirable. Security methods for wireless and wired networks are no different. Many detailed discussions of network security already exist. However, in brief, next section will discuss one alternative based on a virtual private network (VPN) using advanced encryption techniques.

Virtual Private Networks and Encryption

Virtual private networks have been developed to provide high security for confidential data transmissions over public networks, such as the Internet. This method of security has gained wide acceptance and is being extensively used by corporations that wish to provide access to their corporate data networks to employees in remote offices or those traveling without using expensive leased lines. This technique lends itself well to wireless LANs as well. A virtual private network ensures security through both user authentication and encryption. While data encryption is often touted as the sole solution to additional security for wireless LANs, it offers many potential areas for unauthorized users to gain information and thus access the system: transmission of user id and password in the clear and unauthorized access allowing probing of unprotected devices. More importantly, it is arguable whether the encryption techniques defined in wireless LAN standards today are sufficiently strong. With user authentication in the system, not only will the user name and password be encrypted, but access is also controlled through source destination, time, application, and even content filters. The legality of the log-on location is checked and the MAC address may be verified as valid. In addition, where allowed, strong encryption methods such as RC5 are 3-DES are recommended to protect the integrity of the data.

Summary

In this article the design and security issues of the Ad Hoc networks have been presented. Ad Hoc Networks represents a new approach to IP host mobility that incorporates a number of important cellular system features such as passive connectivity, paging, and seamless handoff. The Cellular IP in Ad Hoc network’s routing, handoff, paging, and security algorithms are simple and scalable, resulting in the development of highly scalable software base stations using off-the-shelf PC hardware, operating systems, and radios. Ad Hoc networks can provide a high level of security.
through its use of fluctuating frequency, security ID, and authentication techniques. In addition, considerable effort has to be made to design the system in such a way as to prevent the discovery of the security ID either directly from the hardware or over the air. Depending on user needs, additional security in the form of user authentication and encryption may be employed to more completely protect the Ad Hoc networks. However, a number of challenges remain. Further work is required to extend the protocol and network with suitable quality of service provisioning to support mobile multimedia. Here I believe that Ad hoc network has the fundamental hooks to deliver wireless differentiated services [19] to mobile hosts. More work is required to analyze the network response to link and node failure. Issues of particular interest are the consistency of routes after failure and the time to reestablish route after failure. Further research is required to support multiple gateways in Cellular IP networks. In multiple gateway access networks, a Cellular IP mobile host will use the IP address of one of the gateways as its care-of address and should be capable of changing gateways during normal operations if need be. More emphasis should be laid on providing a secured environment to the user which is free from hassles of Eavesdropping and Intrusions from external element.

References


Publications of Author

Ø WAP Analysis And Design.
   Presented at TECHKRITI 2001 – A National Technical festival at Indian Institute of Technology Kanpur, INDIA in February 2001. It was selected as one of the TOP 5 research works over there.

Ø A Distributed Location Tracking and Call Accounting System for Mobile and Non Mobile Users.
   Completed as a part of research summer project at Dept. of Computer Science and Engineering in May-July 2001. Under process to be presented at CIT- an international conference to be held in Bhubaneswar in December 2001.