

◆ 911-NOW: A Network on Wheels for Emergency Response and Disaster Recovery Operations

David Abusch-Magder, Peter Bosch, Thierry E. Klein,
Paul A. Polakos, Louis G. Samuel, and Harish Viswanathan

Public safety organizations increasingly rely on wireless communication technology to provide effective command, control, and communication during emergencies and disaster response operations. Since emergencies can vary in scale from day-to-day operations to large-scale and widespread catastrophic events, any previously deployed network infrastructure may not be able to handle the traffic load. Worse, the wireless infrastructure may be damaged or destroyed, as occurred during the events of 9/11 and Hurricane Katrina. The 911-network on wheels (911-NOW) solution is a novel portable cellular system based on base station routers (BSRs) that does not require any pre-existing wireless infrastructure and provides capacity and coverage on demand. It is an auto-configurable system with a fully integrated service architecture that can be deployed as a single-cell solution for local communication or be configured to operate as an ad hoc network of cells. This paper describes the 911-NOW vision and discusses some of the differentiating features such as auto-configuration, network management, wireless mesh networking, and interoperability with existing public safety systems. We also highlight some of the research challenges associated with mobile and rapidly deployable wireless networks. In particular we provide an overview of issues centered upon dynamic assignment and management of Internet Protocol (IP) addresses, online and real-time calculation and maintenance of routing information, mobility management, and dynamic configuration and optimization of radio parameters.

© 2007 Alcatel-Lucent.

Introduction

Public safety organizations and law enforcement agencies increasingly rely on wireless communication technology to provide effective command, control, and communication during emergencies and disaster response operations. However, the events of 9/11

brought to light the deficiencies of current communication capabilities when first responders from different agencies and organizations were unable to communicate and exchange critical and potentially life-saving information. This inability to communicate

Panel 1. Abbreviations, Acronyms, and Terms

1x EV-DO—1x evolution–data optimized	IP—Internet Protocol
911-NOW—Network on wheels for emergency response and disaster recovery	ISM—Industrial, scientific, and medical
AHAA—Ad hoc address autoconfiguration	LMR—Land mobile radio
AODV—Ad hoc distance vector routing	MAC—Medium access control
AP—Access point	MANET—Mobile ad hoc networks
ARP—Address Resolution Protocol	MSC—Mobile switching center
ATM—Asynchronous transfer mode	NAT—Network address translation
BSC—Base station controller	ODACP—Optimized Dynamic Address Configuration Protocol
BSR—Base station router	PDSN—Packet data serving node
BTS—Base transceiver station	PN—Pseudo-noise
CDMA—Code division multiple access	QoS—Quality of service
COW—Cell on wheels	RAN—Radio access network
DAAP—Dynamic Address Allocation Protocol	RF—Radio frequency
DACP—Dynamic Address Configuration Protocol	RNC—Radio network controller
DHCP—Dynamic Host Configuration Protocol	SAODV—Secure ad hoc distance vector routing
DSR—Dynamic Source Routing	SEAD—Secure efficient distance vector routing
GGSN—Gateway GPRS support node	SGSN—Serving GPRS support node
GPRS—General packet radio service	SRP—Secure Routing Protocol
GSM—Global System for Mobile Communications	TCP—Transmission Control Protocol
HMMWV—High mobility multipurpose wheeled vehicle	TETRA—Terrestrial trunked radio
HSDPA—High-speed downlink packet access	UDP—User Datagram Protocol
IEEE—Institute of Electrical and Electronics Engineers	UMTS—Universal Mobile Telecommunications System
	VoIP—Voice over IP
	Wi-Fi—Wireless fidelity
	WiMAX—Worldwide interoperability for microwave access

was in part related to the lack of interoperability between different wireless radio systems being deployed. In addition, much of the surrounding wireless and wireline network infrastructure was destroyed or severely damaged. As a result the remaining infrastructure was severely overloaded as first responders, rescue personnel, and the general public were all attempting to access the network and make calls. The deficiencies realized during the events of 9/11 were further emphasized during hurricanes Katrina and Rita when much of the communication infrastructure was damaged, destroyed, or unavailable, and first responders did not have adequate replacement communication capabilities. The size of the affected area during the hurricane disasters was large and spanned several Gulf Coast states, resulting in large-scale and widespread communication deficiencies that required an extensive replacement network.

In general, emergencies faced by public safety and law enforcement agencies can vary in scale from fairly routine and local day-to-day operations to large-scale and widespread catastrophic events. To address the entire scope of possible emergencies, one would have to build networks for the worst-case scenario (assuming we even knew exactly what the worst case scenario would be) and deploy such networks throughout the entire jurisdiction. Such an approach is clearly inefficient and prohibitively expensive. Even worse, the network may still not address communication needs during emergencies as the network itself is exposed to the disaster or may be a target of a man-made disaster. The communication network, rather than aiding in the response, may become the weakest link in our ability to quickly and effectively respond to the emergency.

From recent experience we have learned that first responders, emergency management, and law

enforcement agencies cannot rely on any existing network infrastructure to satisfy their communication needs in times of crises. It is therefore our view that a more efficient approach is to build a mobile, scalable, flexible, and self-sufficient communication network that can be adapted to the level of the emergency. Such a rapidly deployable network should provide reliable and consistent communication capabilities independently of when or where the emergency happens.

When considering solutions for emergency response networks, two broad directions are possible for choosing the underlying radio technology. One approach is to use third generation commercial mobile cellular wireless technologies, such as evolution–data optimized (1x EV-DO) or Universal Mobile Telecommunication System (UMTS), as well as wireless fidelity (Wi-Fi) or worldwide interoperability for microwave access (WiMAX) technologies. The alternate approach is to develop an air-interface technology specifically for emergency networks such as land mobile radio (LMR) or terrestrial trunked radio (TETRA). Employing commercial technology provides significant benefits:

- Wide availability of commercial handsets during emergencies,
- Significant cost savings from economies of scale because of large-scale deployment of commercial technologies,
- Rapid evolution and feature development in handset capabilities and services driven by competition in the commercial market, and
- Multi-vendor interoperable solutions.

Hence, our vision for an emergency network is based on commercial air-interface technology, rather than the proprietary, customized, and special purpose technologies used today, to allow the first responder and public safety community to leverage the ongoing technology evolution and investments in commercial networks.

Since a conventional cellular radio access network comprises multiple network elements, one can envision different alternatives for providing a mobile network solution:

1. In a first solution, only the antennas and the cell sites are mobile and simply provide mobile connection points. Such solutions are currently being

deployed and are usually referred to as cells on wheels (COWs). However, they suffer from their continued reliance on a fixed radio access network infrastructure and backhaul connectivity to the fixed infrastructure. Therefore this solution approach cannot provide reliable communication capabilities (even locally around the deployment area) in certain emergency situations and disasters when the fixed network infrastructure is destroyed or the backhaul connectivity is not available.

2. In a second approach, some (or all) of the network control elements in a traditional wireless architecture could be converted into mobile elements. In code division multiple access (CDMA) networks, for example, these elements include the base transceiver station (BTS), the radio network controller (RNC), the mobile switching center (MSC), and the packet data serving node (PDSN). The corresponding elements in a UMTS network include the node B, the RNC, the serving GPRS support node (SGSN), and the gateway GPRS support node (GGSN). This approach, while providing the necessary functionalities and a full stand-alone network, is not very practical. Indeed, the lack of scalability, the large associated cost, the number of different network elements being deployed, and the limited portability/mobility of the solution make it unattractive for rapid deployment in emergency situations.
3. A more appealing solution for a rapidly deployable wireless network is a fully integrated solution that combines all the functionalities described in the previous solution, but in a single network element that is specifically designed and optimized for a mobile deployment scenario. This network integration, however, brings about a fundamental change in the network architecture from a centralized and hierarchical architecture to a distributed and flat architecture. Indeed, a number of radio resource and mobility management functionalities, traditionally performed by central controllers such as the RNC, now have to be distributed across the network elements.

The 911-NOW solution follows the third approach and provides a novel portable cellular system based on base station routers (BSRs) [2] that does not

require any pre-existing wireless infrastructure and provides capacity and coverage on demand. It is an auto-configurable system with a fully integrated service architecture that can be deployed as a single node solution for local communication or be configured to operate as an ad hoc network of nodes.

The remainder of the paper explores the benefits and technical requirements of such a solution. We provide some background information on the evolution of radio access network architectures, the base station router (BSR), and its motivation and advantages. The vision behind the 911-NOW network solution is then described, along with an overview of its differentiating features. Finally, we provide details of some of the main components of the 911-NOW system, focusing on the auto-configuration of autonomous and rapidly deployable wireless networks.

Evolution of Radio Network Architecture

In this section, we elaborate on the ongoing evolution of radio access network (RAN) architectures from hierarchical and centralized architectures to distributed and flat architectures. The main reason for deploying centralized network architectures is that a central controller (typically the RNC) can manage multiple base stations and efficiently support the mobility and handoff of terminals between different base

stations. This is especially important in second and third generation wireless networks that support soft handoff of mobile terminals to improve the voice capacity of the network. A typical centralized RAN (e.g., for an EV-DO network) is shown in **Figure 1**.

Correspondingly, wireless local area networks, such as those based on the IEEE 802.11 standards, are data-centric and rely on distributed architectures, as illustrated in **Figure 2**. In this architecture, the access point (AP) is responsible for both the air interface and the connection to the mobile terminal, as well as the network connectivity to the Internet.

The current evolution in cellular radio access networks is to migrate from a centralized architecture to a distributed architecture. This trend is driven by the demand for ever-increasing data rates, resulting in numerous cell sites and ever-smaller cell sizes. One of the main objectives of this architectural evolution is to harness the benefits of the core Internet Protocol (IP) philosophy while maintaining the benefits of proven air interface technologies for wide area network deployments. Moving the network intelligence to the edge of the network leads to performance gains by making use of the knowledge and awareness of the wireless channel. In addition, consolidating the radio access network functionalities increases network efficiency by decreasing transmission and processing

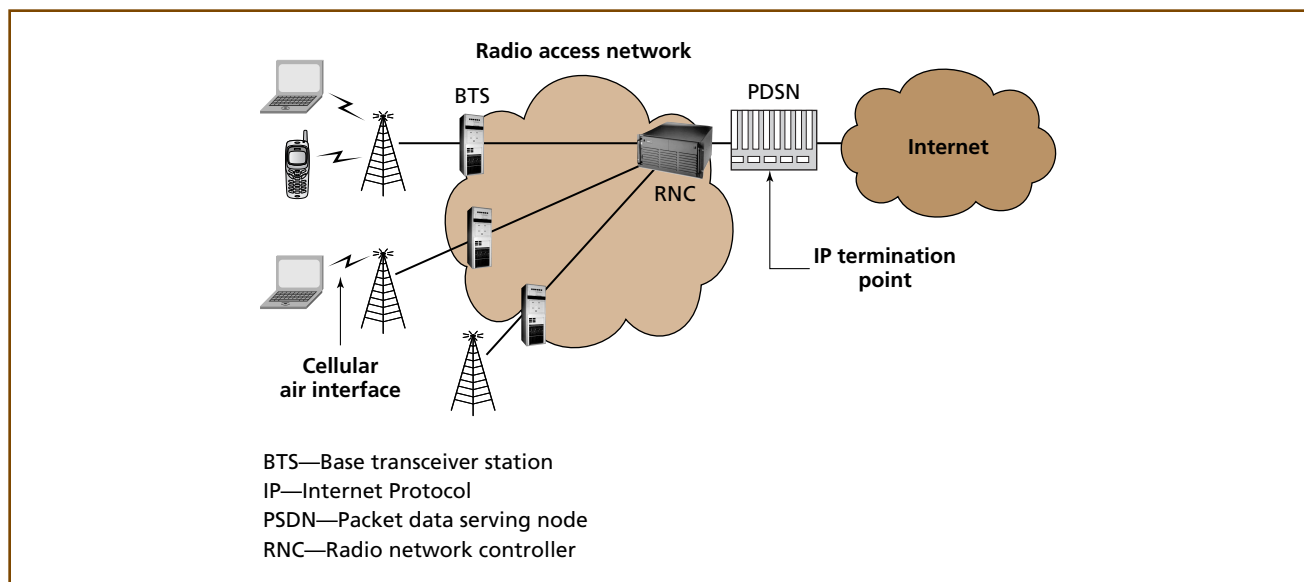


Figure 1.
Centralized architecture for cellular radio access networks.

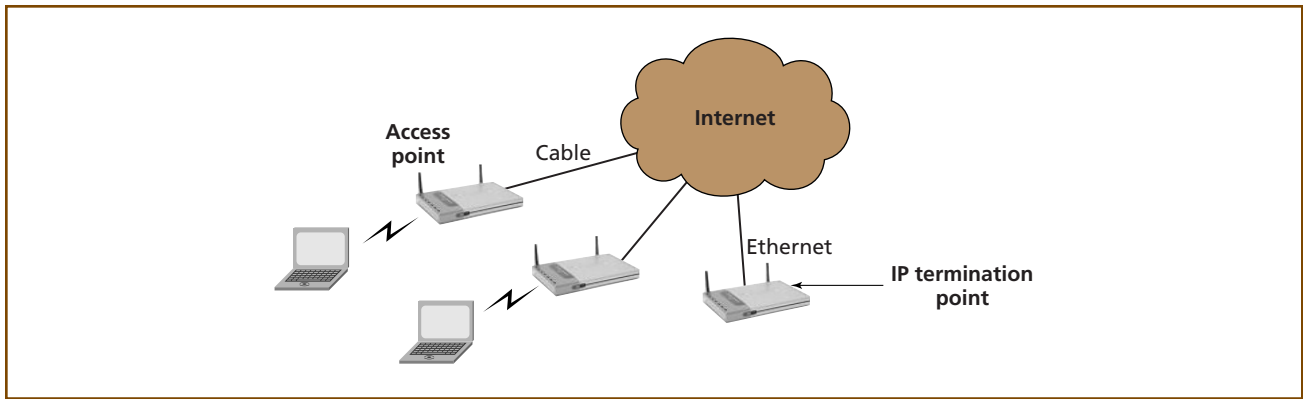


Figure 2.
Distributed architecture for wireless local area networks.

delays in the radio access network, thereby achieving greater network capacity. In order to evolve the network architecture described in Figure 1 to that described in Figure 2, the network functionalities of the BTS, the RNC, and the PDSN all need to be combined in a single network element, called the base station router. Accordingly, the radio resource and mobility management functionalities are now distributed in the network and co-located with each BSR, as illustrated in **Figure 3**.

The main advantages of a distributed architecture are by now well understood and documented in the literature. They include:

1. *Simplicity.* Integrating functionalities leads to deployment of fewer network element types, reduced maintenance and troubleshooting, and significant concomitant cost reductions.
2. *Flexibility.* A single network architecture can be employed and managed independently of the air interface technologies being used. Furthermore,

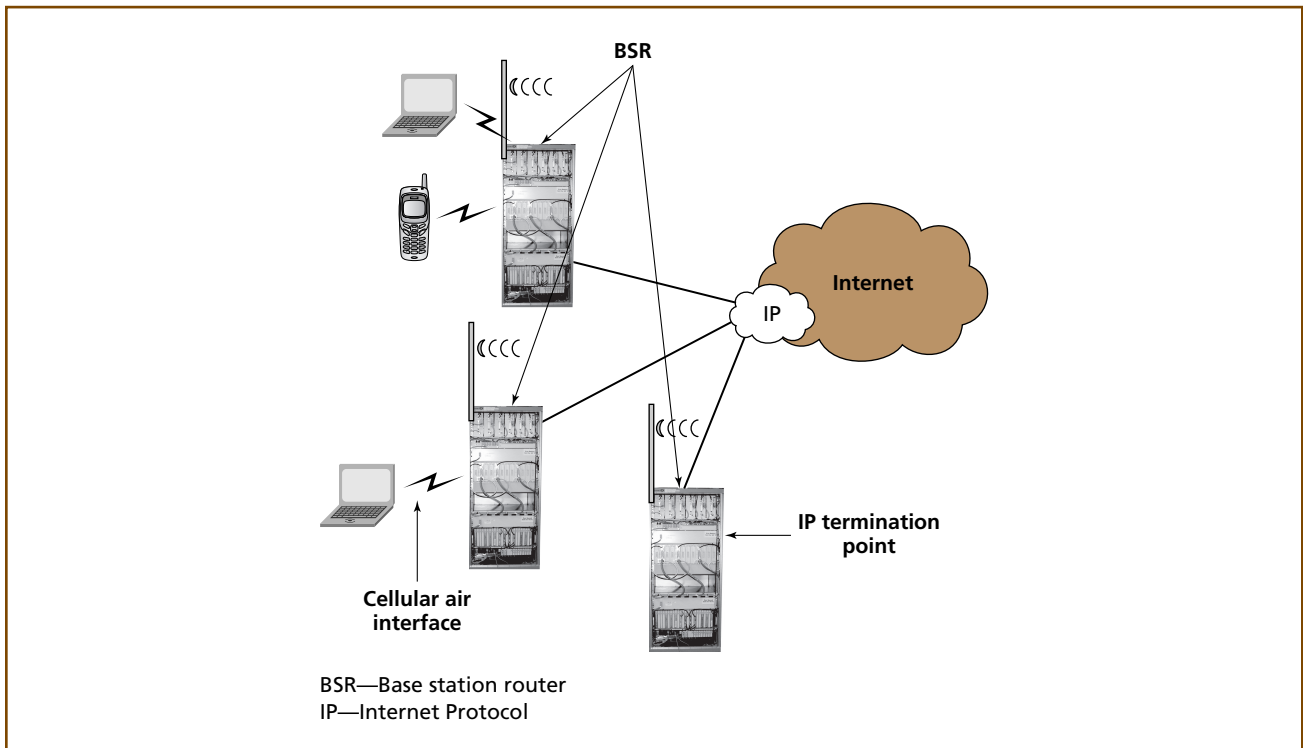


Figure 3.
Distributed all-IP architecture for cellular wireless networks.

the architecture is amenable to different deployment scenarios, including macro cells for wide area coverage, micro cells for hotspot coverage, and pico cells for in-building coverage.

3. *Scalability.* Because of the absence of central controller elements, the architecture can easily be scaled to the required size. In other words, the deployment of additional access points or base stations does not entail the deployment of additional central controllers and a possible redesign of the RAN.
4. *Interoperability.* The proposed architecture essentially decouples the evolution of the air interface technology and the network infrastructure. In other words, the evolution of the air interface is not hampered or tied to the network infrastructure, and vice versa. Through the use of standardized IP interfaces, inter-operability between different networks (possibly deployed by different emergency response agencies and first responder units) is achieved.
5. *Performance.* The integration of different network functionalities leads to the collapse of the protocol stack in a single network element and thereby eliminates transmission delays between network elements and reduces the call setup time and packet fragmentation and aggregation delays. Furthermore, the ability to implement cross-layer optimizations provides additional performance enhancements and resulting capacity gains. Finally, local communication between mobile terminals connected to the same base station is optimized through direct routing at the base station router.

Overview of 911-NOW Network Solution

In this section, we describe the vision of the 911-Network On Wheels (911-NOW) solution and highlight several of the main features. We illustrate some of the main advantages of this novel framework by some sample deployment scenarios.

911-NOW Vision

The vision of the 911-network on wheels (911-NOW) solution is to enable first responders and emergency management teams to communicate

mission-critical information on a secure and rapidly deployable wireless network. To address the requirements imposed on future emergency response networks, the 911-NOW vision provides:

- Assured access and reliable communication anywhere and at any time;
- Capacity and coverage on-demand for mobile incident area networks;
- Efficient local communication in the absence of any fixed and previously deployed network infrastructure;
- Integrated service architecture for full stand-alone network operation;
- Cost-efficient solution that is scalable and flexible to the emergency response needs and the spatial and temporal network deployment scenario;
- Wide area coverage through wireless mesh networking for deployment of jurisdictional area networks;
- Reliability and robustness through flexible multipath routing;
- Wireless backhaul capabilities to a fixed private or public network;
- Converged multimedia communication capabilities with voice, video, and high speed data to enable increased situational awareness at the emergency site; and
- Standards-compliant air interfaces technologies and network interoperability through IP interfaces.

911-NOW Features

The 911-NOW vision leverages the concepts and developments of the base station router. The integrated functionalities and corresponding form factors make the BSR a very attractive solution for a mobile network solution. In **Figure 4**, a sample network deployment scenario is shown that exhibits some of the main appealing features of the 911-NOW network solution:

1. *Land-, sea-, and air-based platform.* Conceptually, the 911-NOW should be compact enough to be mounted on a variety of different platforms, such as fire trucks, high mobility multipurpose wheeled vehicles (HMMWVs or humvees), boats, aerostats, and unmanned drones. The inherent mobility of the network solution allows first

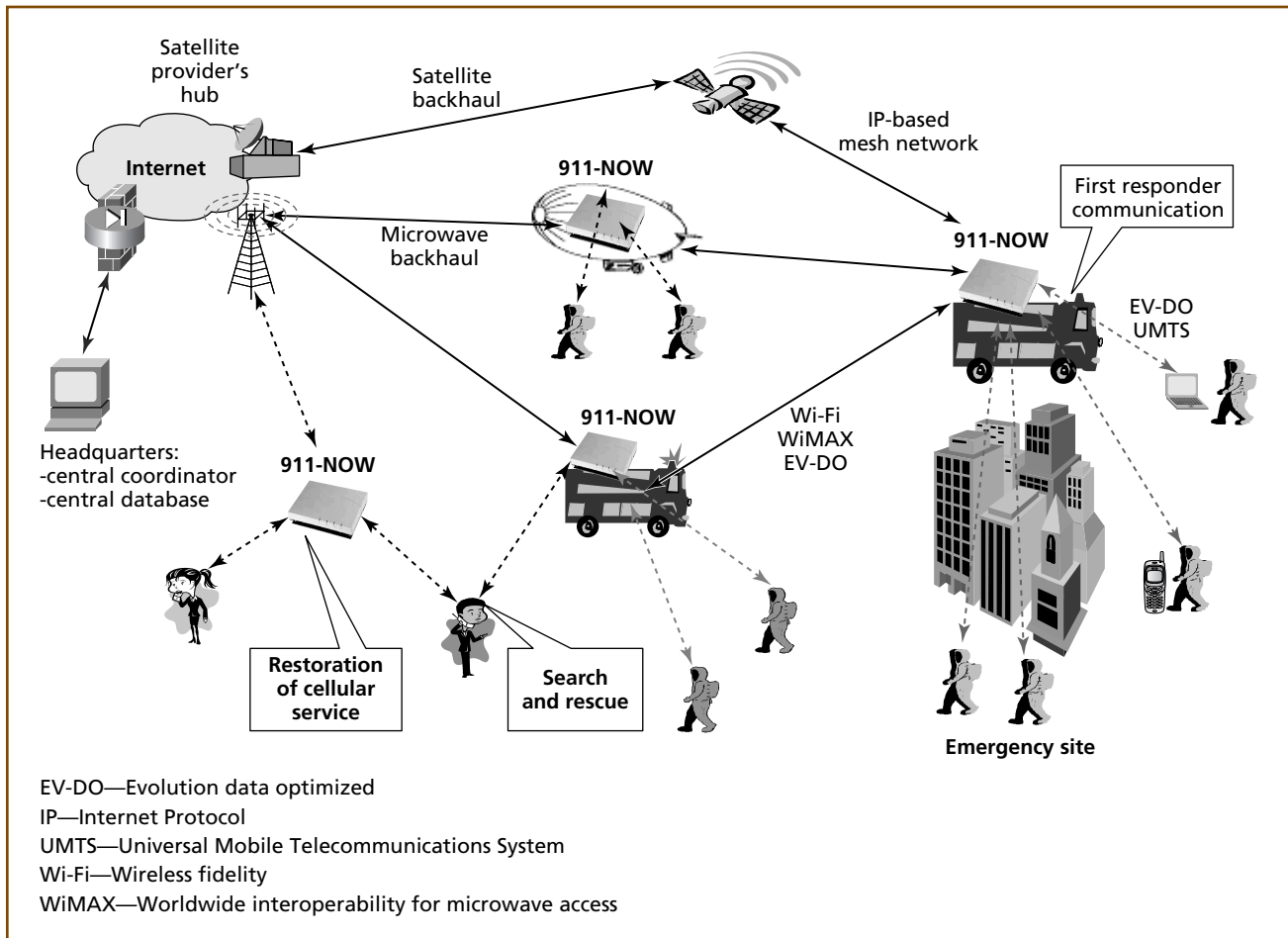


Figure 4. 911-NOW: A mobile network for emergency response and disaster recovery operations based on proven air interface technologies and all-IP networking.

responders, emergency management teams, and tactical units to quickly and flexibly deploy the 911-NOW when and where it is needed, thereby providing capacity and coverage on demand and in real time.

2. *Self-configuration.* The 911-NOW is a turnkey solution with minimum human intervention. Once deployed at the emergency site, the 911-NOW is self-configurable in its setup procedure, IP address assignment, local network topology discovery, local and backhaul network configurations, selection of appropriate transmission parameters, radio resource allocation, and mobility management of mobile terminals. Each 911-NOW is a fully integrated stand-alone network that provides local communication, as well as backhaul

connectivity to the wide area network and the Internet.

3. *Multi-hop and mesh networking capabilities.* If multiple 911-NOW units are deployed, they may be interconnected to form a wireless mesh network for wide area coverage and connectivity. In addition, the mesh network increases the reliability of the network by providing multiple redundant communication paths through the network.
4. *Air interface.* The 911-NOW solution is amenable to any air interface technology, and in a full deployment scenario it is envisioned to provide support for multiple air interfaces, including Global System for Mobile Communications* (GSM*), 1x EV-DO, UMTS, or IEEE 802.16/WiMax. Similarly, the network solution is agnostic of the frequency

spectrum used and the available bandwidth and can be re-banded depending on the expected deployment scenario (e.g., public safety spectrum or commercially available spectrum through licensing agreements). However, only specific technology/bandwidth combinations are feasible; typical bandwidths used for wireless broadband systems range from 1.25 MHz to 20 MHz. Since the 911-NOW BSR is built on standards-compliant and commercially available air interface technologies, the capacity and coverage are identical to those of commercial systems. For example, a UMTS-based solution with 5 MHz of available bandwidth can maintain about 80 simultaneous voice calls and each deployed BSR can achieve peak downlink data rates up to 14.4 Mbps.

5. *Applications.* The 911-NOW may be deployed in support of multiple missions in emergency response and disaster recovery operations. These include, but are not limited to, first responder communications and search and rescue operations, as well as fast restoration of local cellular service. In such scenarios, the applications that are most likely to be needed are basic voice communication through Voice over IP (VoIP), push-to-speak, database access, and file transfer (e.g., access to/downloading of floor plans, emergency exits, elevator shafts, chemical storage rosters, and hazardous material handling databases), alert messaging broadcast, streaming video, location tracking of vehicles and emergency personnel, and sensors (e.g., temperature, air composition, or radiation sensors to detect any abnormalities or changes in the environment), and biometric monitoring applications (e.g., breathing, pulse, and oxygen tank sensors that transmit information about the health of the emergency workers).
6. *Security.* The 911-NOW system provides triple-layered wireless network security to protect the network operator, the mobile terminals, and the network elements. Cryptographic authentication, air interface complexity, encryption, and scrambling, as well as state-of-the-art link layer assisted security protocols, provide a comprehensive set of advanced security tools for strong wireless

security to deter technical fraud, information eavesdropping, and session hijacking.

Coverage and capacity requirements for a jurisdictional area emergency network during a natural disaster or large-scale terrorist attack are significantly different from those of an incident area network required for providing communication capabilities to a localized emergency situation. However, we envision deploying the same 911-NOW solution in both scenarios and leveraging the inherent scalability of the network solution to adjust the communication capabilities to the required level. Appropriate modifications may have to be made to increase the capacity and the coverage of the 911-NOW solution. This could be achieved by deploying a multi-carrier network solution and increasing the transmit power of each 911-NOW unit (through internal or external power boosters). These changes are primarily at the individual BSR level and do not impact any of the networking concepts.

911-NOW Sample Deployment Scenarios

In this section, we highlight the advantages of the 911-NOW solution through several sample deployment scenarios and a comparison with the corresponding deployments in traditional centralized network architectures.

The first scenario of interest involves communication between first responder units deployed around the emergency site and a central coordinator or a database located at the emergency headquarters (i.e., communications between mobile units and a fixed host connected to the Internet). **Figure 5** represents the traditional centralized architecture. **Figure 6** provides a view of communication paths from a mobile unit to headquarters (or any correspondent host connected to a private intranet or the public Internet) using the 911-NOW architecture. Figure 6a depicts a single hop in the wireless backhaul, while Figure 6b shows multiple hops for the wireless backhaul. In both of these architectures, the wireless backhaul link is based on a microwave backhaul. Alternatively, a satellite backhaul link could be considered. This option would be desirable if the wired infrastructure is compromised or not available, if the distances that

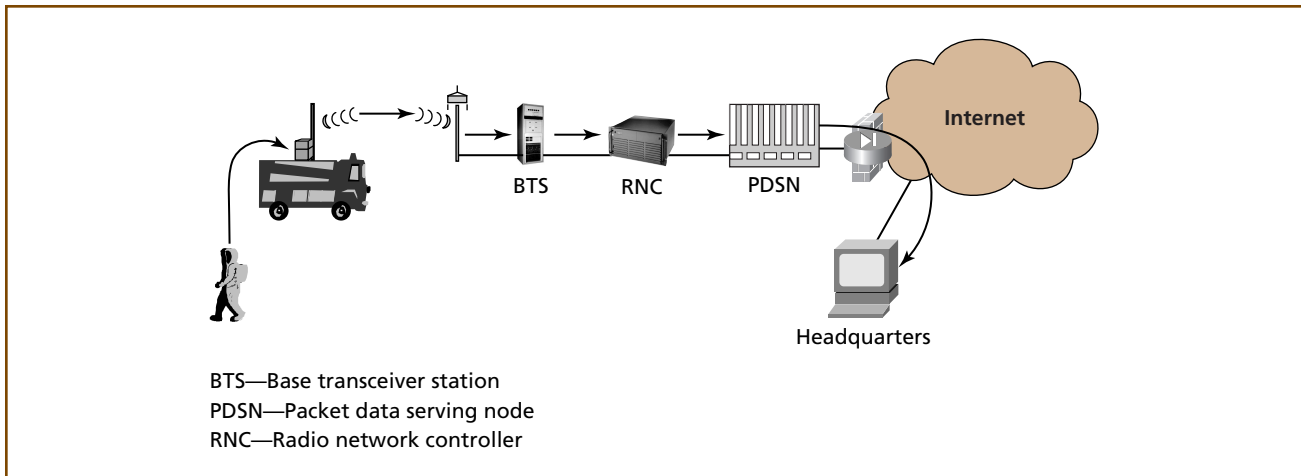


Figure 5. Communication path from a mobile unit to headquarters (central database and coordinator) in the centralized architecture.

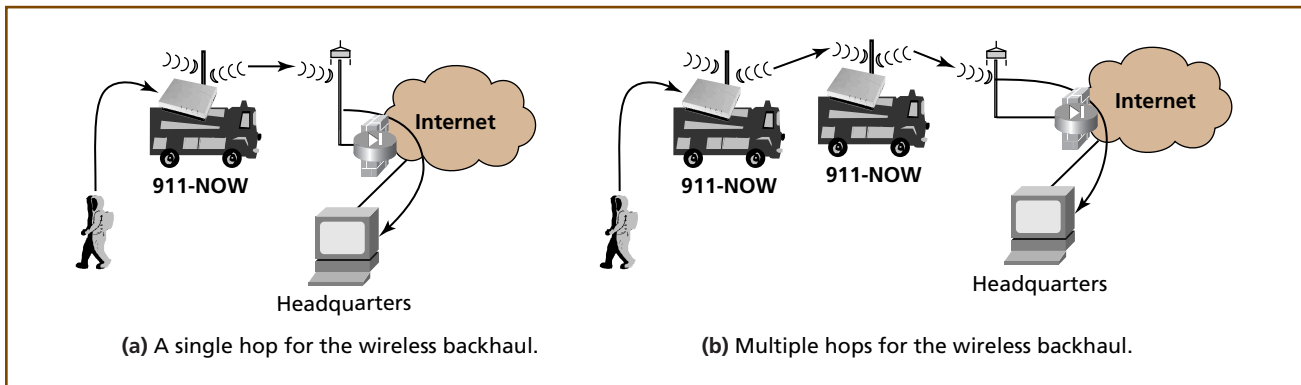


Figure 6. Communication paths from a mobile unit to headquarters using the 911-NOW architecture.

need to be covered for the backhaul connection are too large, or if there is no line-of-sight connection available for the microwave option.

As a second deployment scenario, we consider the communication path between different mobile units deployed around the emergency site. This discussion addresses the essence of the 911-NOW network and the key benefit over the traditional centralized architecture. **Figure 7** and **Figure 8** show a range of communication paths. Indeed, as illustrated in **Figure 7**, even if the mobile units are located close to each other and connected to the same base station, the communication path in the traditional architecture still involves the wired infrastructure in the RAN, since the PDSN is the IP termination

point. Communication would not be possible if this infrastructure were compromised, destroyed, overloaded, or otherwise unable to handle the traffic load. In contrast, the 911-NOW architecture depicted in **Figure 8a** allows local communication independently of the presence of a wired infrastructure, since IP terminates directly at the BSR. Note that the 911-NOW system, by virtue of the multi-hop and mesh networking capabilities shown in **Figure 8b**, allows broader connectivity and communication between mobile units even if they are not in close proximity. The 911-NOW network solution is a flexible solution that can provide scalable capacity and coverage as the needs arise through additional deployments of 911-NOW units.

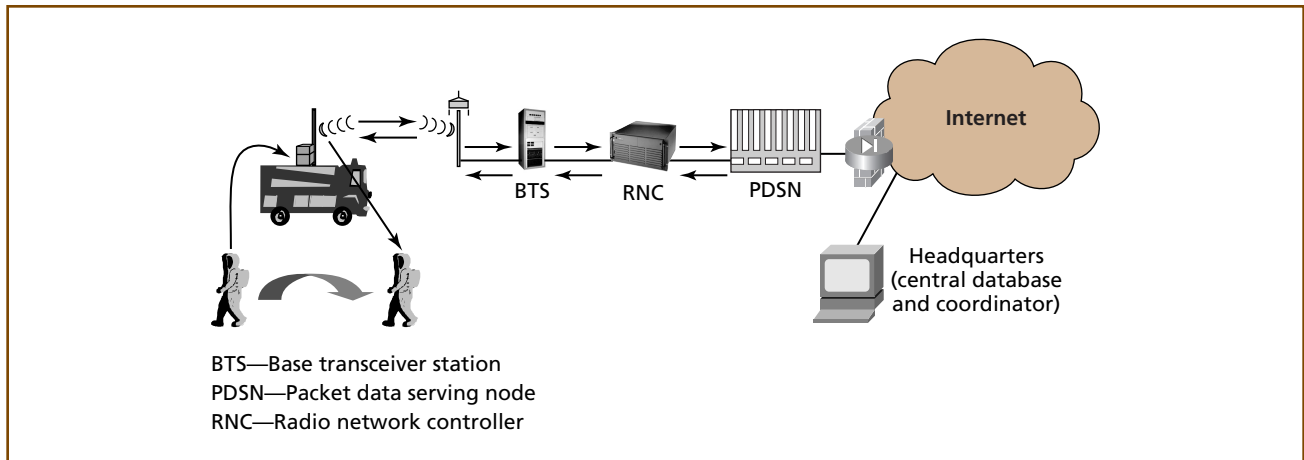


Figure 7.
Communication paths between mobile units in the centralized architecture.

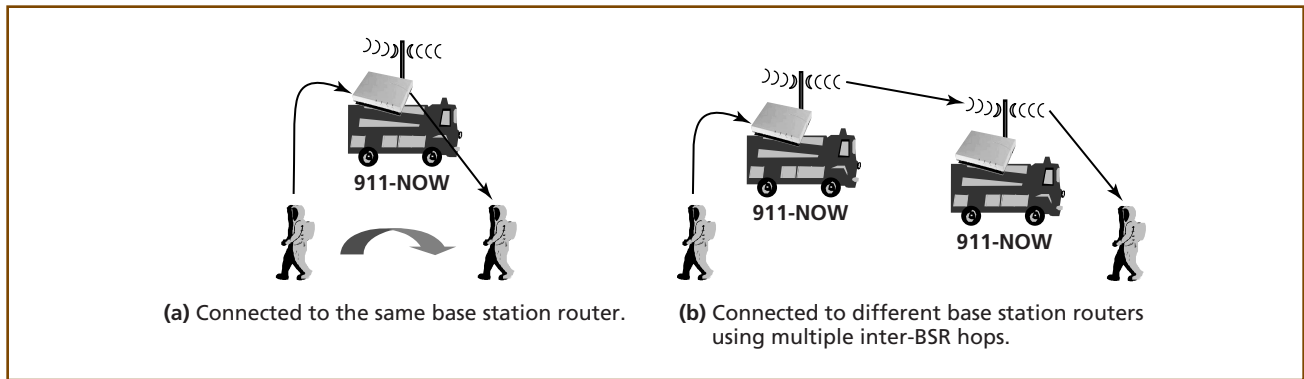


Figure 8.
Communication paths between mobile units in the 911-NOW architecture.

Research Components

In this section, we describe some of the novel features that need to be added to the base station router to enable autonomous and rapid deployment of the 911-NOW network solution. Most of the issues addressed in this section center around auto-configuration of wireless ad hoc and wireless mesh networks. However, we point out that additional challenges beyond the ones highlighted in this paper may need to be addressed before deployment of a complete solution can be envisaged.

Dynamic Assignment and Management of IP Addresses

Before network nodes and mobile terminals can start communicating with each other and with correspondent hosts located on a fixed private or public network, they need to be assigned proper IP addresses. These addresses are used both to identify the nodes

and terminals and to route data traffic to and from the nodes. Therefore it is vitally important that nodes have valid addresses that uniquely identify them, and that the correct routes to the nodes are established in a timely and efficient manner. It is imperative that nodes have unique addresses; otherwise, traffic destined for one of the nodes could be routed to another node. This would lead to confusion and possible instability in the network, compromised traffic and network integrity, and degraded application layer performance—which all may threaten mission success. Preventing address conflicts and duplicate address assignment is especially challenging in networks with varying network topology. Hence, the address management mechanism needs to be robust enough to handle network merges, partitions, remerges, and network node additions and deletions. At the same time, the assigned addresses need to be locally and

globally routable. In other words, network nodes and mobile terminals in the autonomously deployed network need to be able to communicate with and route traffic to each other. In addition, the autonomous network needs to be reachable from a correspondent host located outside the autonomous network, such as a private network or the public Internet. The latter presents an interesting challenge since emergency networks could be deployed anywhere without any a priori knowledge of the location of the emergency.

One possible option to assign addresses is to configure statically the IP addresses for all the nodes (including the base station routers and the mobile terminals) ahead of time. This solution is extremely simple and does not require any real-time configuration procedures. However, this approach would not work in our network scenarios for several reasons. First of all, the assigned addresses may not be globally routable and do not have any relation to the fixed sub-network to which the autonomous wireless network would be connected. Second, conflict-free address assignment cannot be guaranteed since it is not always known a priori which nodes and which mobiles are being deployed; hence, a simple static address allocation is not guaranteed to produce unique routable addresses.

Dynamic address assignment strategies generally fall into one of three categories: leader-based approaches, distributed approaches, and best effort approaches. In leader-based approaches, individual nodes obtain valid IP addresses from a trusted central node with a global view of the network. These approaches include the Dynamic Address Configuration Protocol (DACP) [20], in which nodes obtain addresses in a distributed fashion through a network-wide address request message. The selected address is then registered with a central address authority that maintains a table of the assigned addresses and is responsible for detecting network merges and partitions. In the Optimized Dynamic Address Configuration Protocol (ODACP) [21], the selected address is registered and verified with the central address authority without a network-wide flooding to all the nodes, thereby reducing the signaling overhead in the network. The Dynamic Address Allocation Protocol (DAAP) [16] employs a distributed leader strategy in

which each node becomes the leader until a new node joins the network. Finally, the Dynamic Host Configuration Protocol (DHCP) [5] can also be regarded as a leader-based address assignment mechanism. DHCP provides the capability to assign IP addresses to hosts in the network automatically while guaranteeing that the addresses assigned are unique. The addresses are assigned only for a specific period of time and hence are reusable. Address assignment in DHCP is centrally managed at the DHCP server, and configuration messages between the server and the DHCP clients located at the hosts are based on the Bootstrap Protocol and hence can be conveyed by relay agents. All leader-based approaches suffer from the requirement that a leader needs to be selected, creating a potential bottleneck for signaling traffic as well as a single point of failure. Mechanisms need to be devised to distribute the leader functionality and reduce the signaling overhead. These mechanisms themselves add to the complexity and the network management overhead and consume valuable processing and memory resources in the network nodes.

On the other hand, distributed approaches do not rely on any specific network node to take a leadership role. For example, in the ad hoc address autoconfiguration (AHAA) procedure [18], addresses are randomly selected and explicit duplicate address detection is performed to verify the uniqueness of the address. This mechanism does not, however, consider dynamic network topologies, and since the addresses are randomly selected, they need not be topologically correct and globally routable. In configuration of hosts in a mobile ad hoc network (MANETconf) [11], all the network nodes maintain a list of all the assigned IP addresses in the network, and a new node obtains its address by querying an existing node, which performs a network-wide query on behalf of the requesting node. Other approaches include the buddy approach [23], in which each node maintains a set of IP addresses. If a new node joins the network, an existing node assigns an address to the new node and allocates half of its set of addresses to the new node.

The distributed approaches all suffer from a large signaling overhead, since network-wide queries or broadcasts are required to all the nodes in the network to verify the uniqueness of the assigned

addresses. The methods, therefore, do not scale well in medium to large networks with an increasing number of terminals and nodes [21]. This is particularly true for methods that require explicit address acknowledgments. Furthermore, if explicit address acknowledgments are required from all the nodes, denial of service attacks through false address blocking cannot be prevented. New assignment strategies are needed to eliminate or reduce the vulnerability of the network to denial of service attacks. Since mobile terminals are typically battery powered, any excess signaling and processing reduces the lifetime of the battery and the usability of the device during the emergency. The available set of addresses needs to be specified ahead of time. As a result, topologically correct and globally routable addresses cannot be guaranteed. Depending on the size of the network, the set of addresses may not be large enough. Any nodes that join when all addresses are exhausted cannot be assigned an address and therefore cannot join the network. Such a situation is clearly unacceptable in emergency response networks.

Other approaches are discussed in [6, 21, 22, 26]. Best effort address assignment mechanisms have been suggested in [24, 25, 28], but some of these mechanisms only provide weak duplicate address detection, which allows for duplicate addresses but ensures that packets are routed to the correct destination. The challenge remains to assign and manage globally routable addresses given the mobility of the terminals and the limited address space available to the address assigning authority. Some of these challenges are managed by assignment schemes that are described in the literature. However, the state of the art does not fully address all the functionalities in a single approach that would be applicable to emergency networks. We propose a novel advanced address assignment mechanism. For local communication in an autonomous network, addresses are assigned on the basis of a modified link local address management protocol [3] with an additional feature that enables mobile network nodes to function as proxies for mobile terminals in the network. In the link local address management protocol, a mobile host randomly picks an address and advertises the

address over the link layer. Mechanisms are defined to prevent reuse of existing addresses and to resolve address collisions when two link layer networks are merged into a single link layer network. Address Resolution Protocol (ARP) messages are used to determine medium access control (MAC) addresses corresponding to IP addresses and vice versa. In the hybrid network architecture, a single logical link layer network is created over the multiple node physical network, and the link local addressing method is used to assign unique addresses to all of the hosts in the entire network. To reduce the processing overhead and the broadcast signaling over the air interface, we propose to employ proxy ARP messages with each mobile network node acting as the proxy for mobile hosts connected to it. An ARP cache will be maintained at each network node, which maps the mobile host MAC identities to corresponding IP addresses. Each network node responds to ARP requests on behalf of mobile hosts connected to it and forwards ARP requests to neighboring network nodes if it does not have sufficient information to respond to the ARP request.

When the autonomous wireless emergency response network has a backhaul connection to a fixed or wireless private network or the public Internet, the network node that provides that connection is called the gateway network node. The gateway network node obtains a globally routable address through queries to a DHCP server on the fixed network. This IP address is used for all communication to and from the autonomous network. All internal communication can still be handled by the link local addresses. However, in addition to the DHCP client, the gateway network node is augmented with network address translation (NAT) functionality [10]. The NAT functionality provides a translation between the globally routable address of the gateway network node and the link local address in the autonomous network. Internal communication to the autonomous network has to bypass the NAT functionality; that requires careful implementation so that the NAT functionality is only selectively applied depending on the source and destination of the communication.

Calculation and Maintenance of Routing Information

While a significant amount of research has already been done on ad hoc networks in general, most of the work has concentrated on routing algorithms. The most common routing algorithms for ad hoc networks are the ad hoc on-demand distance vector (AODV) routing [19] and the dynamic source routing (DSR) [9] algorithms. Other routing protocols are described in [13, 15, 17]. Secure versions of the routing protocols have been proposed, such as the secure efficient distance vector routing for mobile ad hoc networks (SEAD) [7], the secure ad hoc distance vector routing (SAODV) [27], or the Secure Routing Protocol (SRP) [14]. However, these solutions are not tailored to the specific requirements of the emergency network that the 911-NOW system seeks to address.

The first, and most important, task of the 911-NOW emergency network is to allow two users, who are both at the scene of the emergency, to communicate with each other. This must be accomplished in the case where both mobile users are associated with a single BSR, and in the case when they are associated with different BSRs that are connected by an ad hoc BSR mesh network. Mobile users in communication with a 911-NOW BSR should also be able to communicate with nodes anywhere on the Internet. In all cases, we wish to ensure quality of service (QoS), and in particular the low latency that is required for effective emergency voice communication. Since mobile devices may associate with and move between any of the 911-NOW BSR elements, the routing and IP-addressing scheme should seek to maintain QoS in the presence of terminal mobility and the changing conditions of inter-BSR links. While any approach adopted for packet routing should scale to the size of the network required for emergency deployments (hundreds or a few thousand BSRs at most), it does not need to scale well for an arbitrarily large-sized network like the Internet. To increase the flexibility of the 911-NOW solution, it is desirable to minimize the requirements on the connection between the 911-NOW network of BSRs and the external network; in particular, this suggests allowing the emergency network to connect to an external network as a client rather than demanding that it be allowed to connect

as a router. These requirements form the basis of the routing solution we propose for use in the 911-NOW system.

The combination of user mobility and the potential addition of BSRs to the mesh network limit the utility of a hierarchical addressing solution for routing in a 911-NOW network. Instead, in our scheme, each mobile terminal receives a unique address (although it is not necessarily a globally routable one, as described in the previous section), and the only hierarchy that is maintained is an association of each mobile device with a particular BSR. A mobile-to-BSR association table is compiled and updates are disseminated throughout the network. By keeping a mobile-to-BSR association table updated, it is possible to quickly find the BSR to which a packet must be delivered for transmission to the mobile terminal, thus reducing packet latency while not relying on any single centralized resource for routing or delivery information. The mobile-to-BSR association table requires modest memory resources (10s of bytes per entry), and while updates require some bandwidth, few other computational resources are required. After a table lookup, the delivery of a data packet from one mobile device to another is reduced to the choice of a route from one BSR to another.

The best approach for route selection from one BSR to another depends on the nature of typical communication patterns. In a 911-NOW system we presume that the most critical (and often used) communication pathways are between two mobile terminals that are within the emergency network. Therefore it is important to have the information to route a packet as directly as possible between two 911-NOW BSRs without necessarily relying on a route passing through a gateway or through some other intermediary node. We also presume that in most scenarios the connectivity of the BSR mesh network is changing on a slower timescale than the typical mobile-to-BSR association time. In that case, separating the mobile-to-BSR association from packet routing and delivery decreases latency and improves QoS. We suggest using a classical approach to routing between BSRs and base our solution on a link state approach, similar to the well-known Open Shortest

Path First and Intermediate System-to-Intermediate System routing protocols. Each time the status of one of the BSR-to-BSR links changes, messages announcing the updated link status flood the system and each of the BSRs recomputes the best possible routes to all other BSRs. Such a link-state routing approach has a cost in bandwidth due to the need to propagate information on changes in link status, and a cost to recompute the routes. However, because of the separation of these two functions, changes in link status can propagate quickly and do not require route re-computation at each step, as would be required in a conventional distance vector routing approach. In this architecture, packets from one mobile user to another are sent to the BSR, then forwarded from BSR to BSR until they reach the BSR associated with the destination mobile device and are finally delivered to the end mobile device. The network connection between BSRs need not be at the network or IP layer; rather, datagrams may be routed and forwarded between BSRs at the link layer, as long as they are delivered to the correct BSR for final delivery to the mobile terminal. This additional flexibility is enabled by the separation of the mobile-to-BSR association from routing decisions, and can help reduce the latency of packet delivery.

To communicate outside the autonomous network, the 911-NOW network requires a connection through a gateway to a broader private or public network. As discussed in the previous section, the gateway serves not only to pass traffic between the two networks, but also to translate between internal 911-NOW addresses and globally routable addresses. To maximize the possibility of connecting a 911-NOW system to a variety of external networks, the gateway is structured as a client of the external network rather than as a router in that network. The client relationship eliminates some of the complications of matching router protocols between the two networks. By eliminating the requirement that the gateway establish a peer relationship with the external network, this approach reduces the trust required for data traffic to flow to the external network. To route incoming packets properly, the gateway must also maintain a mobile-to-BSR association table and participate in the

link-state routing protocol. When a gateway connects to the external network it informs the 911-NOW network of its connection; in this way packets destined for addresses outside the 911-NOW network can be routed to the gateway. In the presence of multiple gateways, the 911-NOW can be configured to route on the basis of the nearest gateway or the external addresses' proximity to a gateway or to match the traffic to the gateway's bandwidth.

Mobility Management

Mobility management in the 911-NOW network is different from mobility management in traditional cellular systems. As described in the previous sections, the 911-NOW system provides a mechanism for communication between a base network element and mobile devices. Clearly, if there is only a single 911-NOW network element in the system, the 911-NOW system does not require any mobility management since a mobile device cannot relocate from one cell to another. In this case, a mobile device is anchored with its physical radio channel, layer 2 radio bearer, and layer 3 endpoint at the 911-NOW BSR.

The 911-NOW emergency network vision is to enable multiple 911-NOW BSRs to organize and configure themselves in an autonomous fashion to operate as a stand-alone and integrated cellular network. However, a key to any cellular network is the support for seamless mobility. This means that when a mobile roams in the area served by another 911-NOW network element, the physical radio channel, layer 2 radio bearer, and layer 3 endpoint need to relocate seamlessly from the original 911-NOW BSR to the new 911-NOW BSR.

Typically in cellular environments, a hierarchy is maintained to support seamless mobility. For instance, a UMTS network provides four network elements to support seamless mobility: a GGSN to provide a layer 3 endpoint, a SGSN to provide layer 3 routing and traffic grooming functionality, and an RNC to provide a layer 2 radio bearer. Finally, a node B (i.e., base station) provides the actual physical radio channel. Similarly, a 1x EV-DO network provides similar network functionalities such as a mobile IP home agent and foreign agent for layer 3 mobility, a PDSN for

header compression and tunneling purposes, and an RNC to hold the layer 2 radio bearer.

The hierarchy in a typical cellular system is maintained to keep the layer 2 radio bearer reasonably static at the RNC while the radio channels are relocated from base station to base station. This means that when channels are relocated, none of the states associated with layer 2 (e.g., the segmentation and re-assembly state, or header compression state) needs to be relocated from cell site to cell site even if the mobile device is moving. Additionally, since the layer 2 radio bearer is almost static, the number of updates required to layer 3 routing is greatly reduced, except for situations when the call is handed off from one RNC to another RNC.

Given that a 911-NOW network is not envisioned to be deployed as a hierarchical system, the 911-NOW system re-uses the mobility techniques from Alcatel-Lucent's base station router. In the BSR architecture [2], mobility is resolved at the cell site level and can just as easily be supported locally as it can with central controllers organized in a hierarchical fashion.

Basically, the BSR provides seamless mobility just as a hierarchical system does: if the hierarchical system relocates a radio channel, so would the BSR. All techniques for radio channel mobility in a standard cellular network are also available in the BSR. The major difference is that the layer 2 radio bearer is not centrally kept. Since the BSR approach requires relocation of the layer 2 radio bearer from BSR to BSR, it also provides a mechanism for frequent layer 3 mobility by informing a mobile IP home agent of the new care-of address for a mobile terminal. The 911-NOW system reuses the BSR's approach for relocation of layer 2 radio bearer and radio channel mobility.

In a sense, the BSR approach does not provide a completely flat system architecture. To support layer 3 mobility, the BSR still requires a central mobile IP home agent to provide IP routing functionality to find a mobile terminal. The BSR does provide a foreign agent. We envision 911-NOW deployments in configurations that cannot support a mobile IP home agent. Thus, to support layer 3 mobility in a 911-NOW network, the 911-NOW system needs to be able

to find layer 2 radio bearers once mobile devices move from one 911-NOW BSR to another.

The 911-NOW system re-uses the ARP mechanism previously discussed for finding mobile devices after their layer 2 radio bearer has relocated from cell site to cell site. Whenever a layer 2 radio bearer relocates, the new cell site issues a gratuitous ARP message on the backhaul network on behalf of the device. This gratuitous ARP message identifies to all of the neighbor 911-NOW BSRs the MAC address of the 911-NOW BSR now serving that particular device. All 911-NOW BSRs that receive the gratuitous ARP message update their ARP cache and thereby update the distributed routing table. Those nodes that do not receive the gratuitous ARP message need to rely on late-binding techniques to find/re-find the layer 2 radio bearer for that particular mobile device.

Cellular systems provide seamless mobility when a radio bearer relocates from cell site to cell site. To support seamless mobility in the 911-NOW system, the 911-NOW BSRs can forward packets to new MAC addresses if they receive an IP packet for a mobile device that has moved to another 911-NOW BSR.

Configuration and Optimization of Radio Parameters

There are some crucial differences between operational commercial cellular and emergency responder networks. A great deal of thought is given to the placement and purchase of antenna sites in commercial cellular networks since it can be an expensive process. Moreover, the RF deployment characteristics change over the lifetime of the deployment. At initial deployment, coverage is a key factor (usually reinforced by regulatory policy). As a network matures and the user numbers increase, the need for coverage transforms into a need for capacity. Because of these characteristics, commercial cellular network deployments tend to be intensively planned with planning tools that utilize empirical or statistical channel propagation models and are operationally confirmed via drive tests.

In stark contrast, an emergency responder network cannot afford to be intensively planned. Its deployment goal is known at inception: that of obtaining maximum coverage with minimum interference.

Although the placement of a mobile emergency responder network has its limitations, there is a great deal of flexibility in placing adjacent nodes to fulfill the coverage requirement. However, it remains very important to have accurate and timely information on the radio network topology before the radio parameters—such as pseudo-noise sequence (PN) offsets, transmit powers, or frequency allocations—can be tuned for optimal network performance. With suboptimal transmission parameters, unnecessary interference may be created that limits the effective data throughput of the network and reduces the capacity of the network. On the other hand, transmit power levels that are too low reduce the coverage of the network and could potentially lead to coverage holes and dropped connections. This is clearly unacceptable in emergency response and disaster recovery networks. We therefore need to determine the radio network topology in an on-line and real-time fashion and adjust the radio parameters accordingly. The nature of the emergency network results in some unique requirements for neighbor discovery and related protocols. We emphasize that the mechanisms developed should be generic and independent of the air interface technologies used to ensure interoperability and communication between different sub-networks.

An important aspect in configuring an ad hoc wireless network is the network topology discovery. There are three distinct notions for measuring the distance between nodes in a wireless multihop network: the hop count on the traffic path between the two nodes, the actual geographical distance between the nodes, and the radio distance based on the wireless channel propagation between nodes. The three metrics are measured in different units and in general can be quite different from each other. In particular, by virtue of the characteristics of wireless communication channels, nodes can be neighbors in the radio sense even if they are not geographically close. Conversely, nodes can be close in geographical distance but be far away from each other in radio distance. This occurs if there are obstructions or buildings along the direct propagation line between the nodes, leading to reduced signal strength at the receiving node. Hence, the metrics used in wired networks for measuring the

distance between nodes are no longer applicable in wireless networks and new metrics and algorithms need to be developed.

Once the radio environment and the channel propagation characteristics are determined, the radio parameters need to be selected and optimized under dynamic network deployment scenarios. By radio parameters, we mean the base station identifications, which are used by mobile terminals to distinguish the transmission from different base stations (such as the PN offsets in CDMA networks) as well as the transmit powers of the base stations.

The PN offsets can be chosen randomly if the deployed network is fairly small since the probability of two different base stations choosing the same PN offset is small. However, protocols need to be implemented to verify that the chosen PN offsets are indeed different. Otherwise, the base stations with colliding PN offsets need to choose different offsets and ensure that there are no overlapping offsets in the radio neighborhood. On the other hand, if the deployed network consists of a larger number of base stations, or if the set of available PN offsets is fairly small, a random allocation will increase the probability of collision. In that case, it would be beneficial to have an optimized distributed assignment mechanism for the PN offsets.

In current cellular networks, the radio parameters are chosen through off-line network optimization techniques after drive test data of the channel propagation environment is collected. Recent work has proposed online optimization algorithms for dynamically selecting these parameters. The concept of autonomic planning of a cellular network was first proposed in [8], and in [1] various algorithms were proposed and evaluated to select the PN offsets based on various levels of information that may be available. Ongoing research efforts investigate similar mechanisms for adjusting the transmit powers of the base stations to minimize the outage probability. The importance of self-deployment and self-configuration of base stations, as well as their impact on future wireless networks, was discussed in [12]. In [4] distributed algorithms for self-deployment and self-configuration are presented and applied to an airport environment

and the achieved performance benefits are described. The transmit powers of the base stations are adjusted to minimize the overall transmit power in the network while ensuring a minimum data rate for all the users. The connections of the mobile terminals to the base stations may continuously be updated as the base station placements and their transmit powers are adjusted. The conditions of the emergency scenario may dictate the placement of the mobile 911-NOW units. First responders have to take logistical and operational conditions and requirements into account when situating the emergency vehicles on which the communication nodes are mounted. However, in certain scenarios, the relative placement of the network nodes may be adjustable and could be optimized so as to increase the efficiency of the network operation further.

The algorithms in [1, 4, 12] form a good basis to develop specific algorithms and protocols for the emergency network scenario. These algorithms can be adjusted for our objective of maximum coverage with minimum interference, while taking into account the information available on the radio network topology. The radio parameter selection algorithms are therefore intimately tied to the radio discovery protocols and the available level of information on the channel propagation environment. The algorithms also depend on how the information is distributed in the network among the base stations and access nodes. We believe that such an integrated approach to network topology discovery, to the distribution of topology information, and to the subsequent radio parameter optimization holds great promise for improved network efficiency and performance. This has not yet been considered in the literature.

Miscellaneous Issues

In this section, we briefly describe a few other issues of importance related to 911-NOW network operation.

Spectrum. An important aspect of any wireless network is the spectrum or frequency band in which the network operates. The concept of an autonomous and rapidly deployable network is agnostic of the spectrum used. However, in a practical context, various spectrum possibilities exist for the operation of

emergency networks such as 911-NOW. One option is to deploy the network in the spectrum that is reserved for wide area public safety networks, such as the 700 MHz to 800 MHz band, which may require re-banding of commercially available handsets. Alternately, it is possible to deploy the network in commercial cellular wireless spectrum owned by wireless service providers. In this approach the service providers would own and operate the emergency network and provide emergency network services to the first responder and emergency management agencies whenever the need arises. Other options include the use of unlicensed spectrum such as the industrial, scientific, and medical (ISM) band. However, transmit power restrictions imply limited range for networks deployed in the unlicensed spectrum.

In the case when the spectrum used is different from the commercial spectrum, radio components used in commercial base stations would have to be modified to be suitable for the chosen spectrum. Specifically, depending on the spectrum used, new duplexers, filters, voltage-controlled oscillators, and power amplifiers are required. Nevertheless, the migration to a new spectrum is not perceived to be a significant challenge.

For the 911-NOW network with mesh interconnections between network nodes, spectrum is also required for the backhaul. If the same spectrum is to be used for both access and mesh backhaul, then a fully flexible physical mesh network may not be feasible. Since cellular access techniques are based on frequency division duplexing, restrictions due to the need for sufficient separation between transmit and receive spectrum will come into play, thereby restricting the meshing capabilities. Hence, separate spectrum for access and backhaul is preferred.

Peer-to-peer capabilities. Current emergency networks possess the capability to do peer-to-peer communications between two end-user terminals without any infrastructure support. Such a feature is likely desirable in any future emergency network as well. The 911-NOW network reuses commercial cellular wireless technology that does not support peer-to-peer capabilities between terminals. To provide such a feature, the terminals can be modified to be

dual-mode terminals, which support both the cellular air interface and another air interface such as Wi-Fi or LMR. The second interface can then be used for peer-to-peer networking. Such dual mode terminals also possess the additional flexibility of providing an alternate access mechanism when the 911-NOW BSRs are not available. These terminals are becoming increasingly common in the commercial wireless market.

Mobile network node interface protocol. One of the important requirements for proper functioning of the 911-NOW network is the protocol interface between the BSRs in the network. This interface is necessary to support the auto-configuration and seamless mobility management capabilities of the network. Auto-configuration requires a protocol similar to the router-to-router protocol in Transmission Control Protocol/Internet Protocol (TCP/IP) networks that incorporates messages for advertisements through which a BSR will inform other BSR nodes of its presence and transmit messages for exchanging configuration parameters as discussed in the previous sections. Mobility management requires mechanisms to exchange handover messages and context transfer schemes for seamless mobility. Such an interface can be designed straightforwardly and can be implemented using User Datagram Protocol (UDP) and TCP as the transport mechanisms.

Conclusions

In this paper, we proposed and described a mobile wireless network infrastructure that is ideally suited for emergency response and disaster recovery operations. Leveraging the base station router framework, which is built on a full integration of all the radio access network functionalities and combines proven air interface technologies with all-IP core networking, the 911-NOW solution is a cost-efficient auto-configurable network that can quickly and easily be deployed. It provides on-demand capacity and coverage with wireless mesh networking capabilities for wide area coverage and network reliability and redundancy. We have highlighted the vision and the differentiating characteristics of the 911-NOW architecture. A detailed description of some of the underlying research issues was provided with an emphasis

on address assignment and management, routing, mobility management and dynamic configuration and optimization of radio parameters.

Acknowledgements

The authors would like to thank an anonymous reviewer for his valuable comments, which have helped improve this paper. The authors also thank Krishan Sabnani and Mark Haner for their encouragement and continued support for this project.

*Trademarks

GSM and Globe System for Mobile Communication are registered trademarks of the GSM Association.

References

- [1] D. Abusch-Magder, A. Y. Chen, K. D. Mirzayans, and H. Viswanathan, "Online PN Offset Planning: An Example of Cellular Network Autoconfiguration," Proc. IEEE Wireless Commun. and Networking Conf. (WCNC '06), (Las Vegas, NV, Apr. 2006).
- [2] M. Bauer, P. Bosch, N. Khrais, L. G. Samuel, and P. Schefczik, "The UMTS Base Station Router," Bell Labs Tech. J., 11:4 (2007).
- [3] S. Cheshire, B. Aboba, and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses," IETF Internet Draft, May 2005, <<http://www.ietf.org/rfc/rfc3927.txt>>.
- [4] H. Claussen, "Autonomous Self-Deployment of Wireless Access Networks in an Airport Environment," Autonomic Communication: Second International IFIP Workshop, WAC 2005, Athens, Gr., Oct. 2005: Revised Selected Papers, (I. Stavrakakis and M. I. Smirnov, eds.), Lecture Notes in Computer Science, Vol. 3854, Springer, Berlin, New York, 2006, pp. 86–98.
- [5] R. Droms, "Dynamic Host Configuration Protocol," IETF RFC 2131, Mar. 1997, <<http://www.ietf.org/rfc/rfc2131.txt?number=2131>>.
- [6] M. Gunes and J. Reibel, "An IP Address Configuration Algorithm for Zeroconfiguration Mobile Multi-Hop Ad Hoc Networks," Proc. Internat. Workshop on Broadband Wireless Ad Hoc Networks and Services (Sophia Antipolis, Fr., 2002).
- [7] L. Ho, Self-Organizing Algorithms for Fourth Generation Wireless Networks and Its Analysis Using Complexity Metrics, Ph.D. Thesis, Queen Mary University of London, Jun. 2003.
- [8] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for

- Mobile Wireless Ad Hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Syst. and Applications (WMCSA '02) (Callicoon, NY, 2002), pp. 3–13.
- [9] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Internet Draft, Jul. 2004, <<http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt>>.
- [10] E. Kohler, R. Morris, and M. Poletto, "Modular Components for Network Address Translation," Proc. IEEE Open Architectures and Network Programming (OPENARCH '02) (New York, 2002), pp. 39–50.
- [11] F. J. Mullany, L. T. W. Ho, L. G. Samuel, and H. Claussen, "Self-Deployment, Self-Configuration: Critical Future Paradigms for Wireless Access Networks," Autonomic Communication: First International IFIP Workshop, WAC 2004, Berlin, Oct. 2004: Revised Selected Papers, (M. I. Smirnov, ed.), Lecture Notes in Computer Science, Vol. 3457, Springer, Berlin, New York, 2005, pp. 58–68.
- [12] S. Murthy and J. Garcia-Lunca-Aceves, "An Efficient Routing Protocol for Wireless Networks," ACM Mobile Networks and Applications J., 1:2 (1996), 183–197.
- [13] S. Nesargi and R. Prakash, "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network," Proc. 21st Annual Joint Conf. of IEEE Computer and Commun. Societies (INFOCOM '02) (New York, 2002), vol. 2, pp. 1059–1068.
- [14] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Commun. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS '02) (San Antonio, TX, 2002).
- [15] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. 16th Annual Joint Conf. of IEEE Computer and Commun. Societies (INFOCOM '97) (Kobe, Japan, 1997), vol. 3, pp. 1405–1413.
- [16] P. Patchipulusu, Dynamic Address Allocation Protocols for Mobile Ad Hoc Networks, M. S. Thesis, Computer Science, Texas A&M University, Aug. 2001.
- [17] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Computer Commun. Review, 24:4 (1994), 234–244.
- [18] C. E. Perkins, J. T. Malinen, R. Wakikawa, E. M. Belding-Royer, and Y. Sun, "IP Address Autoconfiguration for Ad Hoc Networks; Ad Hoc Address Autoconfiguration," IETF Internet Draft, Nov. 2001, <<http://people.nokia.net/charliep/txt/aodvid/autoconf.txt>>.
- [19] C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Workshop on Mobile Computing Syst. and Applications (WMCSA '99) (New Orleans, LA, 1999), pp. 90–100.
- [20] Y. Sun and E. Belding-Royer, Dynamic Address Configuration in Mobile Ad Hoc Networks, Computer Science Dept., University of California Santa Barbara (UCSB), Technical Report 2003–11, 2003.
- [21] Y. Sun and E. M. Belding-Royer, "A Study of Dynamic Addressing Techniques in Mobile Ad Hoc Networks," Wireless Commun. and Mobile Computing, 4:3 (2004), 315–329.
- [22] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," IETF RFC 2462, Dec. 1998, <<http://www.ietf.org/rfc/rfc2462.txt?number=2462>>.
- [23] M. R. Thoppian, A Protocol for Dynamic Configuration of Nodes in MANETs, Master's Thesis, Computer Science, University of Texas Dallas, Aug. 2002.
- [24] N. H. Vaidya, "Weak Duplicate Address Detection in Mobile Ad Hoc Networks," Proc. 3rd ACM Internat. Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '02) (Lausanne, Swit., 2002), pp. 206–216.
- [25] K. Weniger, "Passive Duplicate Address Detection in Mobile Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf. (WCNC '03), (Florence, It., 2003), vol. 3, pp. 1504–1509.
- [26] K. Weniger and M. Zitterbart, "IPv6 Autoconfiguration in Large Scale Mobile Ad-Hoc Networks," Proc. European Wireless 2002 (Florence, It., 2002).
- [27] M. G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. ACM Workshop on Wireless Security (WiSe '02) (Atlanta, GA, 2002).
- [28] H. Zhou, L. M. Ni, and M. W. Mutka, "Prophet Address Allocation for Large Scale MANETs," Proc. 22nd Annual Joint Conf. of IEEE Computer and Commun. Societies (INFOCOM '03) (San Francisco, CA, 2003), vol. 2, pp. 1304–1311.

(Manuscript approved August 2006)

DAVID ABUSCH-MAGDER is a member of technical staff in the End to End Wireless Research Department at Bell Labs in Murray Hill, New Jersey. He received his Sc.B. degree in mathematics/physics from Brown University in Providence, Rhode Island, and his Ph.D. in physics from the Massachusetts Institute of Technology in Cambridge. He was an Alexander von Humboldt Fellow at the University of Munich, and then he joined Bell Labs. During that time Dr. Abusch-Magder has conducted research on silicon single electron transistors; electrical failure in thin insulating films; the electronic properties of nanostructures, polymers, and molecular electronics; and the area of wireless network optimization and design. His current interests include wireless network autoconfiguration and dynamic optimization for future generations of wireless networks, emergency networks, and discrete and continuous algorithms for wireless network optimization.



PETER BOSCH is a member of technical staff at Bell Labs, in Murray Hill, New Jersey. After receiving his Ph.D. in computer science from the University of Twente, Netherlands, he joined the Plan 9[®] operating system group at Bell Labs and later shifted his research interests into wireless systems research. He has worked on the initial prototypes for the base station router (BSR), co-developed the high-speed downlink packet access (HSDPA) demonstrator, and integrated an enhanced mobility procedure for the BSR and is now involved in resolving system architecture evolution/long term evolutions (SAE/LTE) BSR issues. His approach to building a well-integrated cellular system encompasses an end-to-end view of the distributed system—from RF channel to IP-based applications—rather than partitioning the decision and development processes, which can lead to complicated systems that do not work well.



THIERRY E. KLEIN is a member of technical staff in the End to End Wireless Networking Research Department in the Networking and Network Management Center at Bell Labs in Murray Hill, New Jersey. He received both B.S. and M.S. degrees in mechanical engineering from the Université de Nantes in France and an electrical engineering degree in automatics from Ecole Centrale de Nantes in France, where he



ranked first in class. He received the Ph.D. degree in electrical engineering and computer science from the Massachusetts Institute of Technology in Cambridge. Dr. Klein's research interests include information and communication theory, mobility management and resource allocation in wireless networks, as well as end-to-end data performance analysis and cross-layer optimizations. More recently, he has been working on mobile deployable wireless networks with applications toward emergency response, disaster recovery, and tactical operations. He is leading the 911-NOW project within Bell Labs.

PAUL A. POLAKOS is a director of End to End Wireless Networking Research at Bell Labs in Murray Hill, New Jersey. His focus at Bell Labs is physics and wireless research. He has been instrumental in the definition and development of key technology initiatives for digital wireless systems, including intelligent antennas (IA) and multiple input, multiple output (MIMO) Bell Labs Layered Space-Time (BLAST), advanced base station and radio-access-network architectures, radio signal processing, enhancements to wireless networks for high data-rates and high capacity, and dynamic network optimization. He holds B.S., M.S., and Ph.D. degrees in physics from Rensselaer Polytechnic Institute in Troy, New York, and the University of Arizona in Tucson. Prior to joining Alcatel-Lucent, he was actively involved in elementary particle physics research at the U.S. Department of Energy's Fermilab and at the European Organization for Nuclear Research (CERN) and was on the staff of the Max-Planck Institute for Physics and Astrophysics in Munich. He is author or coauthor of more than 50 publications and holds numerous patents.



LOUIS G. SAMUEL is the technical manager of the Global Wireless Systems Research Lab at Bell Labs in Swindon, United Kingdom. Before joining Alcatel-Lucent, he served in the Royal Navy as a nuclear reactor specialist. He studied at Queen Mary and Westfield College, University of London, receiving a master's of communication engineering and a Ph.D. in the application of non-linear dynamics to teletraffic modeling. At Bell Labs he has been involved in the development of advanced protocols and network architectures for wireless communications. His current research interests include non-linear dynamics, complexity theory, agent based systems, software architectures and infrastructures, software protocols,



4G systems, mobility, and resource management. More recently he directed the initial research that led to the base station router (BSR) and the development of flat cellular IP architectures, including heavy involvement in the technology transfer required to make the BSR a product, as well as promotion of the BSR to Alcatel-Lucent customers.



HARISH VISWANATHAN is a distinguished member of technical staff at Bell Labs in Murray Hill, New Jersey. He received the B. Tech. degree from the Department of Electrical Engineering, Indian Institute of Technology, Chennai, and the M.S. and Ph.D. degrees from the School of Electrical Engineering, Cornell University, Ithaca, New York. He was the recipient of the Cornell Sage Fellowship. At Bell Labs, Dr. Viswanathan has worked on multiple antenna technology and other enhancements for third generation wireless, distributed radio network architecture, and next generation wireless technology. His research interests include communication theory, wireless networks, information theory, and signal processing. ◆