Wireless *ad hoc* networking—The art of networking without a network

Magnus Frodigh, Per Johansson and Peter Larsson

Today, many people carry numerous portable devices, such as laptops, mobile phones, PDAs and mp3 players, for use in their professional and private lives. For the most part, these devices are used separately—that is, their applications do not interact. Imagine, however, if they could interact directly: participants at a meeting could share documents or presentations; business cards would automatically find their way into the address register on a laptop and the number register on a mobile phone; as commuters exit a train, their laptops could remain online; likewise, incoming e-mail could now be diverted to their PDAs; finally, as they enter the office, all communication could automatically be routed through the wireless corporate campus network.

These examples of spontaneous, *ad hoc* wireless communication between devices might be loosely defined as a scheme, often referred to as *ad hoc* networking, which allows devices to establish communication, anytime and anywhere without the aid of a central infrastructure. Actually, *ad hoc* networking as such is not new, but the setting, usage and players are. In the past, the notion of *ad hoc* networks was often associated with communication on combat fields and at the site of a disaster area; now, as novel technologies such as Bluetooth materialize, the scenario of *ad hoc* networking is likely to change, as is its importance.

In this article, the authors describe the concept of *ad hoc* networking by giving its background and presenting some of the technical challenges it poses. The authors also point out some of the applications that can be envisioned for *ad hoc* networking.

Introduction

Numerous factors associated with technology, business, regulation and social behavior naturally and logically speak in favor of wireless *ad hoc* networking. Mobile wireless data communication, which is advancing both in terms of technology and usage/penetration, is a driving force, thanks to the Internet and the success of second-generation cellular systems. As we look to the horizon, we can finally glimpse a view of truly ubiquitous computing and communication. In the near future, the role and capabilities of short-range data transaction are expected to grow, serving as a complement to traditional large-scale communication: most man-machine communication as well as oral communication between human beings occurs at distances of less than 10 meters; also, as a result of this communication, the two communicating parties often have a need to exchange data. As an enabling factor, license-exempted frequency bands invite the use of developing radio technologies (such as Bluetooth) that admit effortless and inexpensive deployment of wireless communication.

In terms of price, portability and usability and in the context of an *ad hoc* network, many computing and communication devices, such as PDAs and mobile phones, already possess the attributes that are desirable. As advances in technology continue, these attributes will be enhanced even further.

Finally, we note that many mobile phones and other electronic devices already are or will soon be Bluetooth-enabled. Consequently, the ground for building more complex *ad hoc* networks is being laid. In terms of market acceptance, the realization of a critical mass is certainly positive. But perhaps even more positive—as relates to the end-user—is that consumers of Bluetooth-enabled devices obtain a lot of as-yet unravelled *ad hoc* functionality at virtually no cost.

What is an *ad hoc* network?

Perhaps the most widespread notion of a mobile *ad hoc* network is a network formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. Since the nodes in a network of this kind can serve as routers and hosts, they can forward packets on behalf of other nodes and run user applications.

The roots of *ad hoc* networking can be traced back as far as 1968, when work on the ALOHA network was initiated (the objective of this network was to connect educational facilities in Hawaii).[1] Although fixed

BOX A, ABBREVIATIONS

AODV	*Ad hoc* on-demand distance vector	IP	Internet protocol
AP	Access point	ISM	Industrial Scientific Medical band (2.4 GHz)
ARQ	Automatic repeat request	LAN	Local area network
BGP	Border gateway protocol	LAP	LAN access point
CSMA/CA	Carrier sense multiple access with collision avoidance	MAC	Media access control
		MANET	Mobile *ad hoc* network
DARPA	Defense Advanced Research Projects Agency	MIPMANET	Mobile IP MANET
		MT	Mobile terminal
DSDV	Destination-sequenced distance vector	NC	Notebook computer
		OSPF	Open shortest path first
DSR	Dynamic source routing	PAN	Personal area network
DSSS	Direct-sequence spread spectrum	PDA	Personal digital assistant
		PRnet	Packet radio network
FA	Foreign agent	QoS	Quality of service
FEC	Forward error correction	RIP	Routing information protocol
FHSS	Frequency-hopping spread spectrum	RREP	Route reply
		RREQ	Route request
FTP	File transfer protocol	RTS	Request to send
GPRS	General packet radio service	SIG	Special interest group
H2	See HiperLAN/2	TDD	Time-division duplex
HA	Home agent	UMTS	Universal mobile
IETF	Internet Engineering Task Force	WLAN	Wireless LAN

(Duplicate first page for exhibit labeling, per 37 C.F.R. § 42.63(d)(2)(ii).)

MICROSOFT CORP.
EXHIBIT 1218

Wireless *ad hoc* networking—The art of networking without a network

Magnus Frodigh, Per Johansson and Peter Larsson

Today, many people carry numerous portable devices, such as laptops, mobile phones, PDAs and mp3 players, for use in their professional and private lives. For the most part, these devices are used separately—that is, their applications do not interact. Imagine, however, if they could interact directly: participants at a meeting could share documents or presentations; business cards would automatically find their way into the address register on a laptop and the number register on a mobile phone; as commuters exit a train, their laptops could remain online; likewise, incoming e-mail could now be diverted to their PDAs; finally, as they enter the office, all communication could automatically be routed through the wireless corporate campus network.

These examples of spontaneous, *ad hoc* wireless communication between devices might be loosely defined as a scheme, often referred to as *ad hoc* networking, which allows devices to establish communication, anytime and anywhere without the aid of a central infrastructure. Actually, *ad hoc* networking as such is not new, but the setting, usage and players are. In the past, the notion of *ad hoc* networks was often associated with communication on combat fields and at the site of a disaster area; now, as novel technologies such as Bluetooth materialize, the scenario of *ad hoc* networking is likely to change, as is its importance.

In this article, the authors describe the concept of *ad hoc* networking by giving its background and presenting some of the technical challenges it poses. The authors also point out some of the applications that can be envisioned for *ad hoc* networking.

Introduction

Numerous factors associated with technology, business, regulation and social behavior naturally and logically speak in favor of wireless *ad hoc* networking. Mobile wireless data communication, which is advancing both in terms of technology and usage/penetration, is a driving force, thanks to the Internet and the success of second-generation cellular systems. As we look to the horizon, we can finally glimpse a view of truly ubiquitous computing and communication. In the near future, the role and capabilities of short-range data transaction are expected to grow, serving as a complement to traditional large-scale communication: most man-machine communication as well as oral communication between human beings occurs at distances of less than 10 meters; also, as a result of this communication, the two communicating parties often have a need to exchange data. As an enabling factor, license-exempted frequency bands invite the use of developing radio technologies (such as Bluetooth) that admit effortless and inexpensive deployment of wireless communication.

In terms of price, portability and usability and in the context of an *ad hoc* network, many computing and communication devices, such as PDAs and mobile phones, already possess the attributes that are desirable. As advances in technology continue, these attributes will be enhanced even further.

Finally, we note that many mobile phones and other electronic devices already are or will soon be Bluetooth-enabled. Consequently, the ground for building more complex *ad hoc* networks is being laid. In terms of market acceptance, the realization of a critical mass is certainly positive. But perhaps even more positive—as relates to the end-user—is that consumers of Bluetooth-enabled devices obtain a lot of as-yet unravelled *ad hoc* functionality at virtually no cost.

What is an *ad hoc* network?

Perhaps the most widespread notion of a mobile *ad hoc* network is a network formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. Since the nodes in a network of this kind can serve as routers and hosts, they can forward packets on behalf of other nodes and run user applications.

The roots of *ad hoc* networking can be traced back as far as 1968, when work on the ALOHA network was initiated (the objective of this network was to connect educational facilities in Hawaii).[1] Although fixed stations were employed, the ALOHA protocol lent itself to distributed channel-access management and hence provided a

BOX A, ABBREVIATIONS

AODV	*Ad hoc* on-demand distance vector
AP	Access point
ARQ	Automatic repeat request
BGP	Border gateway protocol
CSMA/CA	Carrier sense multiple access with collision avoidance
DARPA	Defense Advanced Research Projects Agency
DSDV	Destination-sequenced distance vector
DSR	Dynamic source routing
DSSS	Direct-sequence spread spectrum
FA	Foreign agent
FEC	Forward error correction
FHSS	Frequency-hopping spread spectrum
FTP	File transfer protocol
GPRS	General packet radio service
H2	See HiperLAN/2
HA	Home agent
HiperLAN/2	High-performance radio LAN type 2
IEEE	Institute of Electrical and Electronic Engineering
IETF	Internet Engineering Task Force
IP	Internet protocol
ISM	Industrial Scientific Medical band (2.4 GHz)
LAN	Local area network
LAP	LAN access point
MAC	Media access control
MANET	Mobile *ad hoc* network
MIPMANET	Mobile IP MANET
MT	Mobile terminal
NC	Notebook computer
OSPF	Open shortest path first
PAN	Personal area network
PDA	Personal digital assistant
PRnet	Packet radio network
QoS	Quality of service
RIP	Routing information protocol
RREP	Route reply
RREQ	Route request
RTS	Request to send
SIG	Special interest group
TDD	Time-division duplex
UMTS	Universal mobile telecommunications system
WCDMA	Wideband code-division multiple access
WLAN	Wireless LAN

basis for the subsequent development of distributed channel-access schemes that were suitable for *ad hoc* networking. The ALOHA protocol itself was a single-hop protocol—that is, it did not inherently support routing. Instead every node had to be within reach of all other participating nodes.

Inspired by the ALOHA network and the early development of fixed network packet switching, DARPA began work, in 1973, on the PRnet (packet radio network)—a multihop network.[2] In this context, multihopping means that nodes cooperated to relay traffic on behalf of one another to reach distant stations that would otherwise have been out of range. PRnet provided mechanisms for managing operation centrally as well as on a distributed basis. As an additional benefit, it was realized that multihopping techniques increased network capacity, since the spatial domain could be reused for concurrent but physically separate multihop sessions.

Although many experimental packet-radio networks were later developed, these wireless systems did not ever really take off in the consumer segment. When developing IEEE 802.11—a standard for wireless local area networks (WLAN)—the Institute of Electrical and Electronic Engineering (IEEE) replaced the term packet-radio network with *ad hoc* network. Packet-radio networks had come to be associated with the multihop networks of large-scale military or rescue operations, and by adopting a new name, the IEEE hoped to indicate an entirely new deployment scenario.

Today, our vision of *ad hoc* networking includes scenarios such as those depicted in Figure 1, where people carry devices that can network on an *ad hoc* basis. A user's devices can both interconnect with one another and connect to local information points—for example, to retrieve updates on flight departures, gate changes, and so on. The *ad hoc* devices can also relay traffic between devices that are out of range. The airport scenario thus contains a mixture of single and multiple radio hops.

To put *ad hoc* networking in its right perspective, let us make some observations about wireless communication, beginning with present-day cellular systems, which rely heavily on infrastructure: coverage is provided by base stations, radio resources are managed from a central location, and services are integrated into the system. This lead to the good and predictable service of

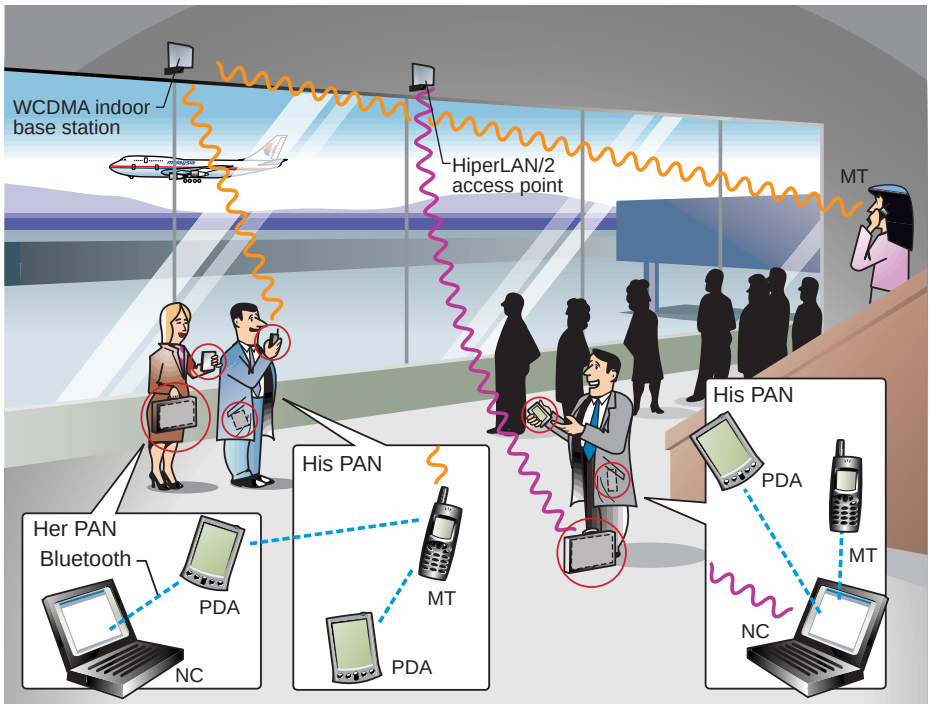


Figure 1.
At an airport, where people can access local- and wide-area networks, *ad hoc* Blutooth connections are used to interconnect carried devices, such as PDAs, WCDMA mobile phones and notebook computers. For instance, a user might retreive e-mail via a HiperLAN/2 interface to a notebook computer in a briefcase, but read messages and reply to them via his or her PDA.

present-day cellular systems. Figure 2 depicts this two-dimensional aspect as it relates to *ad hoc* networking.

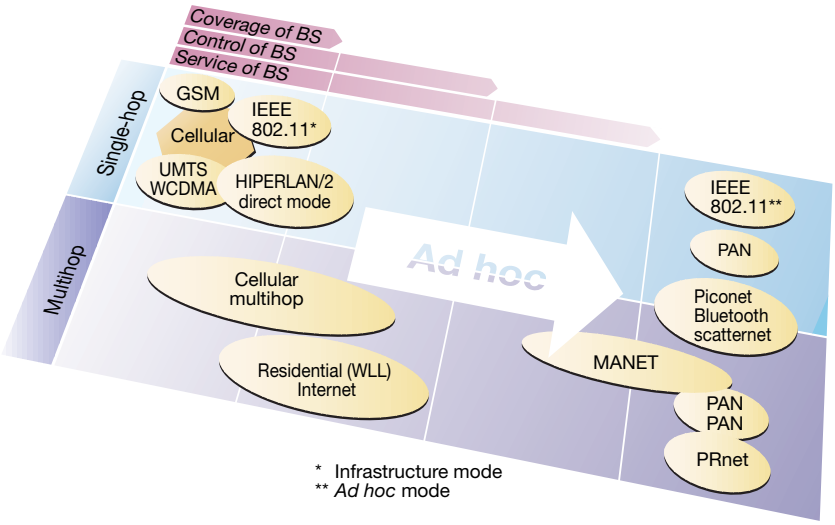
As we decrease, or move away from, central management, we find ourselves moving in the direction of pure *ad hoc* operation, which can also be classified in terms of single or multiple hops.

Without having fully relinquished control, but given the direct mode of communication in HiperLAN/2, adjacent terminals can communicate directly with one another. Thus, the transport of traffic is not entirely dependent on the coverage provided by access points.

Dependency on centrally administered coverage is further reduced when end-user terminals relay traffic in a multihop fashion between other terminals and the base station (cellular multihop).[3] A similar approach applies to commercial or residential wireless local loop (WLL) multihop access systems, primarily conceived for Internet access (Figure 2, bottom left and middle).

Fully decentralized radio, access, and routing technologies—enabled by Bluetooth, IEEE 802.11 *ad hoc* mode, PRnet stationless mode, mobile *ad hoc* network (MANET), and concepts such as the personal area network (PAN) or PAN-to-PAN communication—fit more or less entirely into the *ad hoc* domain. The MANET initiative by the Internet Engineering Task Force (IETF) also aims to provide services via fixed infrastructure connected to the Internet.[4] Recent development and characteristics within this genre are the focus of this article (Figure 2, bottom right).

Figure 2
Various wireless networks mapped to two independent aspects of *ad hoc* networking: the level of centralized control (horizontal), and the use of radio multihopping (vertical).



Typical applications

Mobile *ad hoc* networks have been the focus of many recent research and development efforts. So far, *ad hoc* packet-radio networks have mainly been considered for military applications, where a decentralized network configuration is an operative advantage or even a necessity.

In the commercial sector, equipment for wireless, mobile computing has not been available at a price attractive to large markets. However, as the capacity of mobile computers increases steadily, the need for unlimited networking is also expected to rise. Commercial *ad hoc* networks could be used in situations where no infrastructure (fixed or cellular) is available. Examples include rescue operations in remote areas, or when local coverage must be deployed quickly at a remote construction site. *Ad hoc* networking could also serve as wireless public access in urban areas, providing quick deployment and extended coverage. The access points in networks of this kind could serve as stationary radio relay stations that perform *ad hoc* routing among themselves and between user nodes. Some of the access points would also provide gateways via which users might connect to a fixed backbone network.[5]

At the local level, *ad hoc* networks that link notebook or palmtop computers could be used to spread and share information among participants at a conference. They might also be appropriate for application in home networks where devices can communicate directly to exchange information, such as audio/video, alarms, and configuration updates. Perhaps the most far-reaching applications in this context are more or less autonomous networks of interconnected home robots that clean, do dishes, mow the lawn, perform security surveillance, and so on. Some people have even proposed *ad hoc* multihop networks (denoted sensor networks)—for example, for environmental monitoring, where the networks could be used to forecast water pollution or to provide early warning of an approaching tsunami.[6]

Short-range *ad hoc* networks can simplify intercommunication between various mobile devices (such as a cellular phone and a PDA) by forming a PAN, and thereby eliminate the tedious need for cables. This could

also extend the mobility provided by the fixed network (that is, mobile IP) to nodes further out in an *ad hoc* network domain. The Bluetooth system is perhaps the most promising technology in the context of personal area networking.

PAN—a network extension

Seen from the viewpoint of the traditional mobile network, a Bluetooth-based PAN opens up a new way of extending mobile networks into the user domain. Someone on a trip who has access to a Bluetooth PAN could use the GPRS/UMTS mobile phone as a gateway to the Internet or to a corporate IP network. In terms of traffic load in the network, the aggregate traffic of the PAN would typically exceed that of the mobile phone. In addition, if Bluetooth PANs could be interconnected with scatternets, this capacity would be increased. Figure 3 shows a scenario in which four Bluetooth PANs are used. The PANs are interconnected via laptop computers with Bluetooth links. In addition, two of the PANs are connected to an IP backbone network, one via a LAN access point and the other via a single GPRS/UMTS phone.

A PAN can also encompass several different access technologies—distributed among its member devices—which exploit the *ad hoc* functionality in the PAN. For instance, a notebook computer could have a wireless LAN (WLAN) interface (such as IEEE 802.11 or HiperLAN/2) that provides network access when the computer is used indoors. Thus, the PAN would benefit from the total aggregate of all access technologies residing in the PAN devices. As the PAN concept matures, it will allow new devices and new access technologies to be incorporated into the PAN framework. It should also eliminate the need to create hybrid devices, such as a PDA-mobile phone combination, because the PAN network will instead allow for wireless integration. In other words, it will not be necessary to trade off form for function.

In all the scenarios discussed above, it should be emphasized that close-range radio technology, such as Bluetooth, is a key enabler for introducing the flexibility represented by the PAN concept.

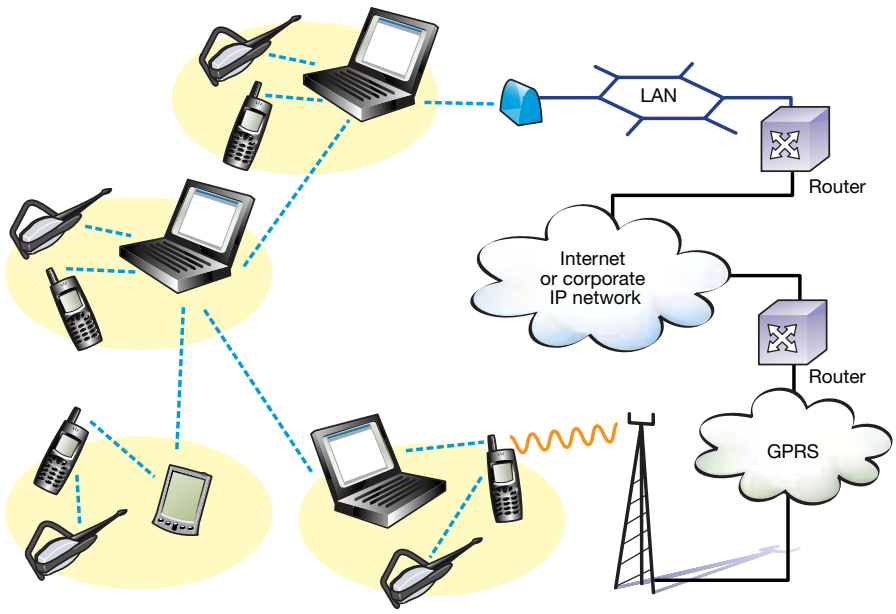


Figure 3
PAN scenario with four interconnected PANs, two of which have an Internet connection via a Bluetooth LAN access point and a GPRS/UMTS phone.

Characteristics and requirements

In contrast to traditional wireline or wireless networks, an *ad hoc* network could be expected to operate in a network environment in which some or all the nodes are mobile. In this dynamic environment, the network functions must run in a distributed fashion, since nodes might suddenly disappear from, or show up in, the network. In general, however, the same basic user requirements for connectivity and traffic delivery that apply to traditional networks will apply to *ad hoc* networks.

Below, we discuss some typical operational characteristics and how they affect the requirements for related networking functions. To limit the scope of the discussion, we will examine the case of a PAN-oriented *ad hoc* network that involves a mix of notebook computers, cellular phones, and PDAs.

- Distributed operation: a node in an *ad hoc* network cannot rely on a network in the background to support security and routing functions. Instead these functions must be designed so that they can operate efficiently under distributed conditions.
- Dynamic network topology: in general, the nodes will be mobile, which sooner or later will result in a varying network topology. Nonetheless, connectivity in

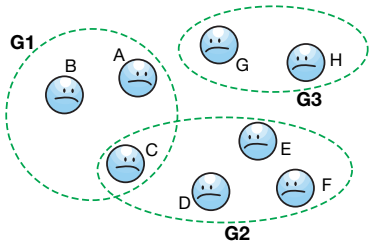


Figure 4
This *ad hoc* network has three separate trust groups: *G1*, *G2* and *G3*. At this stage, a secure exchange of data cannot occur between the nodes—except with node *C*, which belongs to *G1* and *G2*.

the network should be maintained to allow applications and services to operate undisrupted. In particular, this will influence the design of routing protocols. Moreover, a user in the *ad hoc* network will also require access to a fixed network (such as the Internet) even if nodes are moving around. This calls for mobility-management functions that allow network access for devices located several radio hops away from a network access point.

- Fluctuating link capacity: the effects of high bit-error rates might be more profound in a multihop *ad hoc* network, since the aggregate of all link errors is what affects a multihop path. In addition, more than one end-to-end path can use a given link, which if the link were to break, could disrupt several sessions during periods of high bit-error transmission rates. Here, too, the routing function is affected, but efficient functions for link layer protection (such as forward error correction, FEC, and automatic repeat request, ARQ) can substantially improve the link quality.
- Low-power devices: in many cases, the network nodes will be battery-driven, which will make the power budget tight for all the power-consuming components in a device. This will affect, for instance, CPU processing, memory size/usage, signal processing, and transceiver output/input power. The communication-related functions (basically the entire protocol stack below the applications) directly burden the application and services running in the device. Thus, the algorithms and mechanisms that implement the networking functions should be optimized for lean power consumption, so as to save capacity for the applications while still providing good communication performance. Besides achieving reasonable network connectivity, the introduction of multiple radio hops might also improve overall performance, given a constrained power budget. Today, however, this can only be realized at the price of more complex routing.

Given the operating conditions listed above, what can the user expect from an *ad hoc* PAN network? The support of multimedia services will most likely be required within and throughout the *ad hoc* PAN. As an example, the following four quality-of-service (QoS) classes would facilitate the use of multimedia applications including

- conversational (voice);
- streaming (video/audio);
- interactive (Web); and
- background (FTP, etc.).

These service classes have been identified for QoS support in the UMTS network and should also be supported in the PAN environment. However, the inherent stochastic communications quality in a wireless *ad hoc* network, as discussed above, makes it difficult to offer fixed guarantees on the services offered to a device. In networks of this kind, fixed guarantees would result in requirements for how nodes move, as well as requirements for node density, which would inherently inhibit the notion of *ad hoc* operation. Nevertheless, when communication conditions are stable, the PAN infrastructure should provide the same QoS as has been defined for the access network. To further improve user perception of the service, user applications that run over an *ad hoc* network could be made to adapt to sudden changes in transmission quality.

QoS support in an *ad hoc* network will affect most of the networking functions discussed above, especially routing and mobility. In addition, local buffer management and priority mechanisms must be deployed in the devices in order to handle differentiated traffic streams.

In the following section we elaborate more on three of the functions briefly mentioned above, namely, security, routing, and mobility. We believe that these functions are good points of departure for a discussion of the implications that *ad hoc* operation will have on network functionality.

Typical *ad hoc* network functions

Security

Obviously, security is a concern in an *ad hoc* network, in particular if multiple hops are employed. How can a user be certain that no one is eavesdropping on traffic via a for-

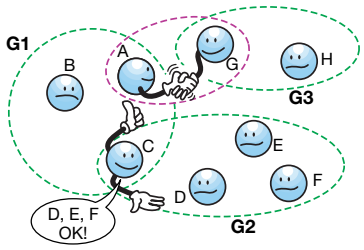


Figure 5
Node *C* sends the signed public keys it received from nodes *D*, *E* and *F* to server node *A*. In addition, node *A* establishes a new trust relationship to node *G*.

warding node? Is the user at the other end really the person he claims to be? From a purely cryptographic point of view, *ad hoc* services do not imply many "new" problems. The requirements regarding authentication, confidentiality, and integrity or non-repudiation are the same as for many other public communication networks. However, in a wireless *ad hoc* network, trust is a central problem. Since we cannot trust the medium, our only choice is to use cryptography, which forces us to rely on the cryptographic keys used. Thus, the basic challenge is to create trusted relationships between keys without the aid of a trusted third-party certification.

Since *ad hoc* networks are created spontaneously between entities that happen to be at the same physical location, there is no guarantee that every node holds the trusted public keys to other nodes or that they can present certificates that will be trusted by other parties. However, if we allow trust to be delegated between nodes, nodes that already have established trusted relationships can extend this privilege to other members of the group.

The method described below can be used for distributing relationships of trust to an entire *ad hoc* network. The method is based on a public key approach and is exemplified by a small *ad hoc* network (Figures 4-7). We assume that connectivity exists between all the nodes in the network, and that it can be maintained by, say, a reactive *ad hoc* routing protocol.

- Initially, node *A* takes on the role of server node in the procedure of delegating trust. *A* triggers the procedure by flooding a start message into the network. Each node that receives this message floods the *ad hoc* network with a message containing the set of trusted public keys. *A* can then establish a "map" of trusted relations and identify them in the *ad hoc* network. In the example shown (Figure 4), three different groups (*G1*, *G2*, and *G3*) share a chain of trust.
- All the nodes in *G2* share an indirect trusted relationship to *A* (through node *C*). Node *A* can thus collect the signed keys it received from *G2* via *C* (as illustrated in Figure 5). By contrast, the nodes in *G3* do not have a trusted relationship to *A*. However, a trusted relationship between, say, node *G* in *G3* and *A* can be created by manually exchanging trusted keys.
- Node *A* can now collect signed keys received from *G3* via *G* (Figure 6). *A* can then flood the *ad hoc* network with all collected signed keys. This procedure creates trusted relationships between every node in *G1*, *G2* and *G3*, and forms a new trust group, *G1'* (Figure 7).

This example can be generalized into a protocol that handles the distribution of trust in an arbitrary *ad hoc* network.[7]

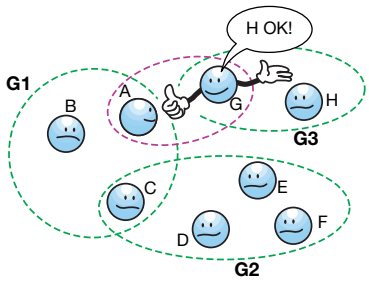


Figure 6
Node *G* sends the signed public key it received from node *H* to node *A*.

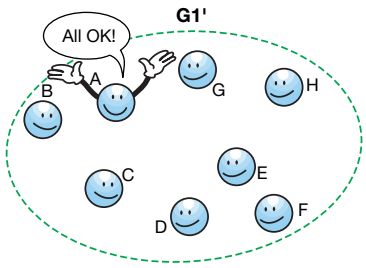
Routing in *ad hoc* networks

For mobile *ad hoc* networks, the issue of routing packets between any pair of nodes becomes a challenging task because the nodes can move randomly within the network. A path that was considered optimal at a given point in time might not work at all a few moments later. Moreover, the stochastic properties of the wireless channels add to the uncertainty of path quality. The operating environment as such might also cause problems for indoor scenarios—the closing of a door might cause a path to be disrupted.

Traditional routing protocols are proactive in that they maintain routes to all nodes, including nodes to which no packets are being sent. They react to any change in the topology even if no traffic is affected by the change, and they require periodic control messages to maintain routes to every node in the network. The rate at which these control messages are sent must reflect the dynamics of the network in order to maintain valid routes. Thus, scarce resources such as power and link bandwidth will be used more frequently for control traffic as node mobility increases.

An alternative approach involves establishing reactive routes, which dictates that routes between nodes are determined solely when they are explicitly needed to route packets. This prevents the nodes from updating every possible route in the network, and instead allows them to focus either on routes that are being used, or on routes that are in the process of being set up.

Figure 7
Node *A* floods the *ad hoc* network with all the signed keys. A new chain of trust is thus created in a new, secure trust group, *G1'*, which comprises all the nodes in the network.



In a simulation study, SwitchLab[8] (Ericsson Research) compared two reactive routing algorithms (*ad hoc* on-demand distance vector, AODV[9], and dynamic source routing, DSR[10]) and one proactive routing algorithm (destination-sequenced distance vector, DSDV[11]) (Box B). In every case tested, the reactive algorithms outperformed the proactive algorithm in terms of throughput and delay. Moreover, the reactive protocols behaved similarly in most of the simulated cases. The main conclusion drawn from this study is that a reactive approach might well be necessary in a mobile environment with limited bandwidth capacity. The proactive approach depletes too many resources updating paths (if the route-update periods are to match the mobility of the nodes). If the update interval is too long, the network will simply contain a large amount of stale routes in the nodes, which results in a significant loss of packets.

Mobility functions

In present-day cellular networks, node and user mobility are handled mainly by means of forwarding. Thus, when a user circulates outside his home network any calls directed to him will be forwarded to the visiting network via his home network. This same forwarding principle applies to mobile IP.[12, 13] A user, or actually the node with the IP interface, can also continue to use an IP address outside the subnetwork to which it belongs. A roaming node that enters a foreign network is associated with a c/o address provided by a foreign agent (FA). In the home network, a home agent (HA) establishes an IP tunnel to the FA using the c/o address. Any packet sent to the roaming node's address is first sent to the home agent, which forwards it to the FA via the c/o address (tunneling). The FA then decapsulates the packet and sends it to the roaming node using the original (home) IP address. The actual routing in the fixed network is not affected by this tunneling method and can use traditional routing protocols such as open shortest path first (OSPF), the routing information protocol (RIP), and the border gateway protocol (BGP). This forwarding approach is appropriate in cases where only the nodes (terminals) at the very edges of (fixed) networks are moving.

However, in an *ad hoc* network, this is not the case, since the nodes at the center of the network can also move—or rather, the whole network is based on the idea of devices that serve both as routers and hosts at the same time. Hence, in an *ad hoc* network, mobility is handled directly by the routing algorithm. If a node moves, forcing traffic another way, the routing protocol takes care of the changes in the node's routing table.

In many cases, interworking can be expected between *ad hoc* and fixed networks. Interworking would make it possible for a user on a trip who takes part in a laptop conference but wants mobility, to be reachable via the fixed IP network. Moreover, since the user wants to be reachable from the fixed network, mobile IP would be a convenient way of making him reachable through the fixed IP network. If the user is located several radio hops away from the access point, mobile IP and the *ad hoc* network routing protocol must interwork to provide connectivity between the travelling user and his

BOX B, THREE MOBILE *AD HOC* NETWORK-ROUTING PROTOCOLS

Destination-sequenced distance vector

DSDV is a proactive hop-by-hop distance vector routing protocol. Each network node maintains a routing table that contains the next hop to any reachable destination as well as the number of hops that will be required. Periodical broadcasts of routing updates are used to keep the routing table completely updated at all times. To guarantee loop-freedom, DSDV uses a concept that is based on sequence numbers to indicate how new, or fresh, a given route is. Route *R*, for example, will be considered more favorable than *R*' if *R* has a higher sequence number; whereas if the routes have the same sequence number, *R* will have the lower, or more recent, hop-count.

Note: in a distance vector (or Bellman-Ford) algorithm, the network nodes exchange routing information with their neighbors. The routing table in a node contains the next hop for every destination in the network, and is associated with a "distance" metric—for example, the number of hops. Based on the distance information in the neighbor's routing tables, it is possible to compute the shortest-path (or minimum-cost) routes to every destination in a finite time for a network with no topology changes.

***Ad hoc* on-demand distance vector**

Like DSDV, AODV is a distance vector routing protocol, but it is reactive. This means that AODV solely requests a route when it needs one, and does not require that the nodes should maintain routes to destinations that are not communicating. AODV uses sequence numbers in a way similar to DSDV to avoid routing loops and to indicate the freshness of a route. Whenever a node needs to find a route to another node, it broadcasts a route request (RREQ) message to all its neighbors. The RREQ message is flooded through the network until it reaches the destination or a node that has a fresh route to the destination. On its way through the network, the RREQ message initiates the creation of temporary route table entries for the reverse route in the nodes it passes. If the destination—or a route to it—is found, its availability will be indicated by a route reply (RREP) message that is unicast back to the source along the temporary reverse path of the received RREQ message. On its way back to the source, the RREP message initiates, in the intermediate nodes, routing table entries for the destination. Routing table entries expire after a certain timeout period.

Dynamic source routing

Dynamic source routing is a reactive routing protocol that uses source routing to deliver data packets. The headers of the data packets carry the addresses of the nodes through which the packet must pass. This means that intermediate nodes need only keep track of their immediate neighbors in order to forward data packets. The source, on the other hand, must know the complete hop sequence to the destination. As in AODV, the route acquisition procedure in DSR requests a route by flooding the system with an RREQ packet. A node that receives an RREQ packet searches its route cache, where all its known routes are stored, for a route to the requested destination. If no route is found, it forwards the RREQ packet after first having added its own address to the hop sequence stored in the packet. The packet propagates through the network until it reaches either the destination, or a node with a route to the destination. If a route is found, an RREP packet containing the proper hop sequence for reaching the destination is unicast back to the source node. Another feature of the DSR protocol is that it can learn routes from the source routes in packets it receives.

unit's peer node, which is located in the fixed network or in another *ad hoc* network.

MIPMANET

Mobile IP for mobile *ad hoc* networks (MIPMANET)[14] is designed to give nodes in *ad hoc* networks

- access to the Internet; and
- the services of mobile IP.

The solution uses mobile IP foreign agents as access points to the Internet to keep track of the *ad hoc* network in which any given node is located, and to direct packets to the edge of that *ad hoc* network.

The *ad hoc* routing protocol is used to deliver packets between the foreign agent and the visiting node. A layered approach that employs tunneling is applied to the outward data flow, to separate the mobile IP functionality from the *ad hoc* routing protocol—Figure 8 illustrates how mobile IP and *ad hoc* routing functionality are layered. This makes it possible for MIPMANET to provide Internet access by enabling nodes to select multiple access points and to perform seamless switching between them. In short, MIPMANET works as follows:

- Nodes in an *ad hoc* network that want Internet access use their home IP addresses for all communication, and register with a foreign agent.
- To send a packet to a host on the Internet, the node in the *ad hoc* network tunnels the packet to the foreign agent.
- To receive packets from hosts on the Internet, packets are routed to the foreign agent by ordinary mobile IP mechanisms. The foreign agent then delivers the packets to the node in the *ad hoc* network.
- Nodes that do not require Internet access interact with the *ad hoc* network as though it were a stand-alone network—that is, they do not require data regarding routes to destinations outside the *ad hoc* network.
- If a node cannot determine from the IP address whether or not the destination is located within the *ad hoc* network, it will first search for the visiting node within the *ad hoc* network before tunneling the packet.

By using tunneling, MIPMANET can incorporate the default route concept into on-demand *ad hoc* routing protocols, such as AODV and DSR, without requiring any major modifications. Packets addressed to destinations that are not found within the *ad hoc* network are tunneled to foreign agents. In MIPMANET, only registered visiting nodes are given Internet access, thus the only traffic that will enter the *ad hoc* network from the Internet is traffic that is tunneled to the foreign agent from a registered node's home agent. Likewise, traffic that leaves the *ad hoc* network is tunneled to the foreign agent from a registered node. This results in a separation between, and thereby the capacity to control, traffic that is local in the *ad hoc* network and traffic that enters the *ad hoc* network.

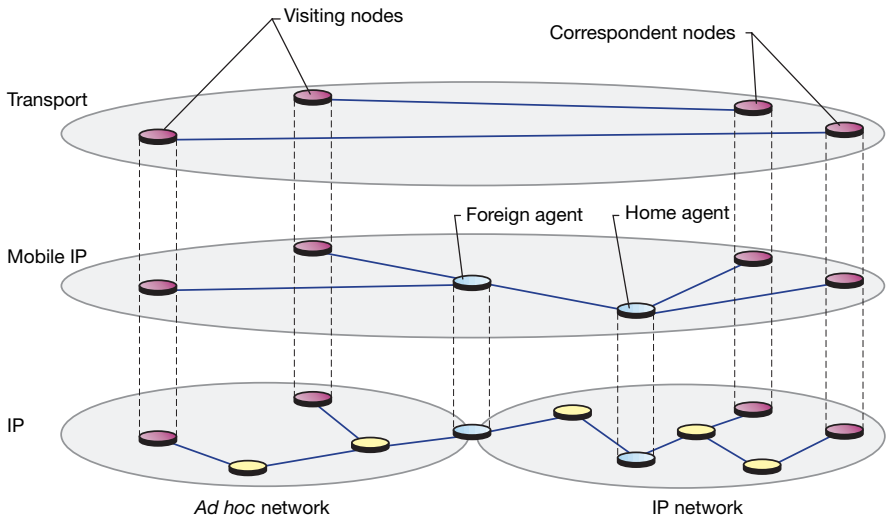


Figure 8
An overview of the MIPMANET architecture.

Radio layer implications

Why multiple hops?

In dealing with an unreliable wireless broadcast medium, special "radio" considerations should be addressed in the communication system of an *ad hoc* network, to ensure reliable and efficient operation. One way of doing this is to employ multihopping, which facilitates the reuse of resources in both the spatial and temporal domains, provided that the nodes which participate in the network are reasonably well distributed in space.[15] In contrast, single-hop networks mainly share the channel resources in the temporal domain. Figure 9 shows a schematic depiction of the spatial interference in multihopping and single-hopping scenarios. Each case considers an identical situation with respect to node distribution, sources, and destinations. In the multihopping scenario, packets are routed

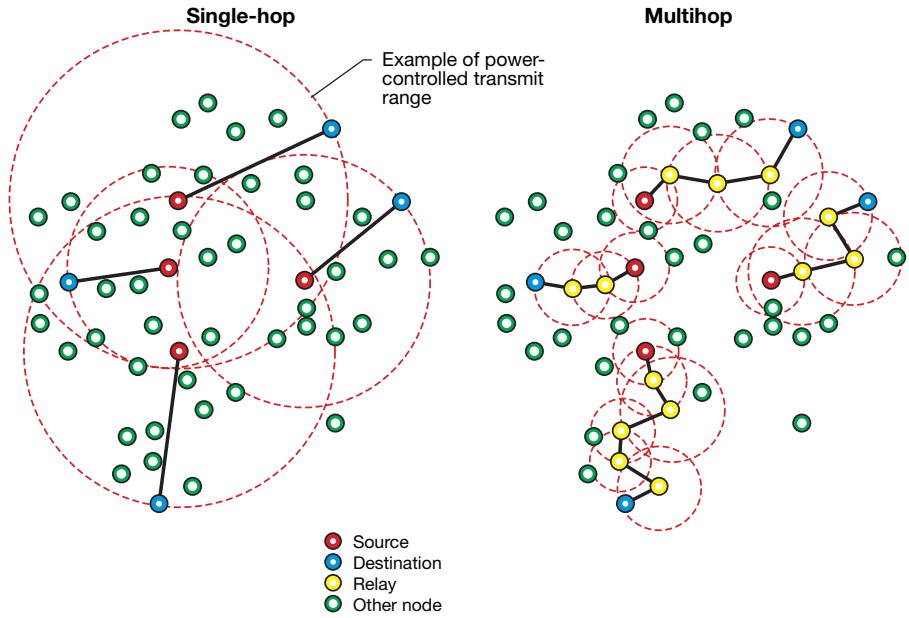


Figure 9
Comparison of multihop networking with single-hop networking. Both examples have an identical distribution of network nodes.

over intermediate relays. However, the single-hop network sends the data directly from the source to destination. The circles in the figure indicate a power-controlled range of the transmitting nodes. The figure also depicts inactive nodes—these nodes are not involved as sources, destinations, or intermediate relays. From this figure, we get the feeling that the multihop scenario provides greater spectral efficiency (bit/s/Hz/m^2).

Comparison of multiple hops and single hops

Whether multihopping is necessary, suitable or even possible depends on factors such as the number and distribution of terminals in the network, relative traffic density, radio channel characteristics, practical communication limitations, and reasons for optimizing certain parameters. Under some circumstances, a multihop network might actually degenerate into a single-hop network. One obvious reason for employing multihopping is to provide connectivity, since some terminals might be out of range of each other, and cannot therefore form a single-hop network.

Multihop characteristics—forwarding

In a multihop scenario, it makes sense not to waste more energy than what each hop requires. In essence, the key to conserving energy is to control the transmit power, in order to compensate for path losses that occur when a message is sent between adjacent nodes.

In a network scenario with little data traffic, the overall power consumption can be reduced by approximately a factor of $N^{\alpha-1}$, where N is the number of equidistant hops between the source and the destination, and α is the propagation constant. In theory, α is equal to 2 for free space propagation. But for realistic environments, it is often assigned a value of 3 or 4. To derive the relationship $N^{\alpha-1}$, we first describe propagation loss (L) in terms of its relationship to distance (R):

$$L = Const \cdot R^{\alpha}$$

For correct reception at a given level of receiver noise, a minimum receiving power PRX_min is required. Accordingly, the transmit power for one hop over distance R is (stated somewhat simplistically):

$$P_{TX_1} = P_{RX_min} \cdot Const \cdot R^{\alpha}$$

If the distance (R) is divided into N hops, then each individual hop requires

$$P_{TX_N} = P_{RX_min} \cdot Const \cdot (R/N)^{\alpha}$$

This is a factor N^{α} less than a long single

hop. Thus, the overall end-to-end reduction in transmit power is

$$\frac{N^{\alpha}}{N} = N^{\alpha-1}$$

In this analysis, we have excluded many detrimental factors, such as unequal hop ranges, retransmissions, and the characteristics of fading channels. Moreover, we have assumed a very simple model of propagation loss. Notwithstanding, the results hint at potential power savings. For example, compared to the single-hop case, given $\alpha=3.5$ and $N=16$, the overall theoretical end-to-end transmit power per packet is reduced by 1000 times, or 30 dB. The bad news is that in a mobile *ad hoc* network

- connectivity usually needs to be maintained between neighbors; and
- routing information needs to be distributed.

Thus, in highly mobile situations, the control traffic required in a multihop network might consume a noticeable amount of energy, even in the absence of data traffic.

A direct benefit of controlling power over short-range transmissions is that it can reduce the total interference level in a homogeneous multihop network with multiple communicating nodes and fixed traffic. In a first approximation—without considering the specific interference location—the average level of interference is reduced by the same amount as the transmit power; that is, by $N^{\alpha-1}$. Furthermore, less interference implies greater link capacity. Given a somewhat crude application of Shannon's bandwidth-limited channel capacity relation, and by assuming that the interference is well modeled with complex Gaussian noise, the individual link capacity increases for large N: $lg(N)$. This is shown below, where B is the bandwidth and SIR_1 is the signal-to-interference ratio for a link in a reference single-hop system that has been replaced with a multihop system:

$$C_{link} = B \cdot lg_2(1 + SIR_1 \cdot N^{\alpha-1}) \approx Const_1 \cdot lg_2(N) + Const_2$$

The end-to-end delay depends on the level at which latency is measured and the applied forwarding principle. A message of reasonable size which is to be forwarded in the store-and-forward manner will experience delay that is proportional to the number of hops. Nonetheless, this delay is compensated for in part by an increase in the link data rate.

The segmenting of large messages into multiple packets also affects the end-to-end delay. By segmenting the message, several packets can be transferred concurrently over consecutive hops. Under those assumptions, the delay imposed by multiple hops is small in comparison to the delay resulting from the link rate and message size. In fact, end-to-end delay might actually benefit from multiple hops. Because traffic can be routed concurrently over multiple links in a "multihop chain," the challenge is to alleviate the associated interference.

Obviously, when transmit power is limited, it might not be possible to reach the desired station without multiple hops. On the other hand, because the maximum size of messages is fixed, too many hops will increase delay. This implies that a given number of hops, N, can provide a minimum delay under transmit power constraints and a given message size.

In summary, multihopping is beneficial, since it

- conserves tranmit energy resources;
- reduces interference; and
- increases overall network throughput.

Multihopping might also be a necessity, to provide any kind of connectivity between very distant terminals.

Bluetooth networking

Worldwide, the industry has shown a tremendous interest in techniques that provide short-range wireless connectivity. In this context, Bluetooth technology is seen as the key component.[16-18] However, Bluetooth technology must be able to operate in *ad hoc* networks that can be stand-alone, or part of the "IP-networked" world, or a combination of the two.

The main purpose of Bluetooth is to replace cables between electronic devices, such as telephones, PDAs, laptop computers, digital cameras, printers, and fax machines, by using a low-cost radio chip. Short-range connectivity also fits nicely into the wide-area context, in that it can extend IP networking into the personal-area network domain, as discussed earlier.

Bluetooth must be able to carry IP efficiently in a PAN, since PANs will be connected to the Internet via UMTS or corporate LANs, and will contain IP-enabled hosts. Generally speaking, a good capacity for carrying IP would give Bluetooth networks a wider and more open interface, which would most certainly boost the development of new applications for Bluetooth.

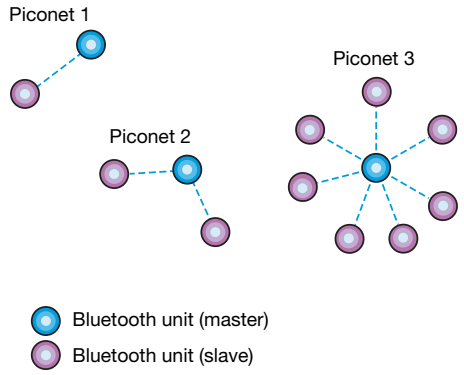


Figure 10
Examples of Bluetooth piconets.

Bluetooth basics

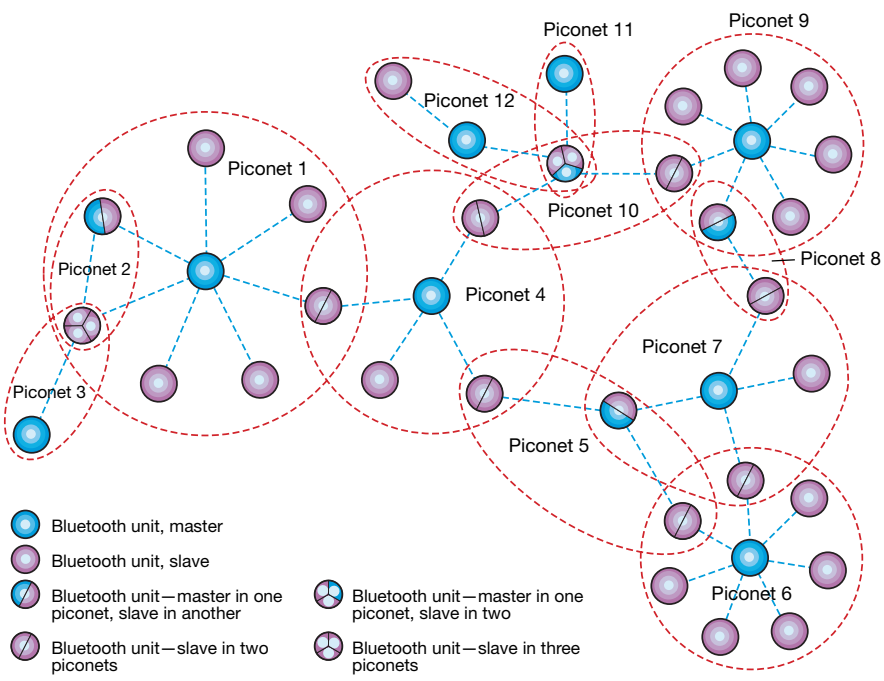
Bluetooth is a wireless communication technology that uses a frequency-hopping scheme in the unlicensed Industrial-Scientific-Medical (ISM) band at 2.4 GHz. Two or more Bluetooth units that share the same channel form a piconet (Figure 10). Within a piconet, a Bluetooth unit can play either of two roles: master or slave. Each piconet may only contain one master (and there must always be one) and up to seven active slaves. Any Bluetooth unit can become a master in a piconet.

Furthermore, two or more piconets can be interconnected, forming what is called a scatternet (Figure 11). The connection point between two piconets consists of a Bluetooth unit that is a member of both piconets. A Bluetooth unit can simultaneously be a slave member of multiple piconets, but only a master in one. Moreover, because a Bluetooth unit can only transmit and receive data in one piconet at a time, its participation in multiple piconets has to be on a time-division multiplex basis.

The Bluetooth system provides duplex transmission based on slotted time-division duplex (TDD), where the duration of each slot is 0.625 ms. There is no direct transmission between slaves in a Bluetooth piconet, only from master to slave and vice versa.

Communication in a piconet is organized so that the master polls each slave according to a polling scheme. A slave is only allowed to transmit after having been polled by the master. The slave will start its transmission in the slave-to-master timeslot immediately after it has received a packet from the master. The master may or may not include data in the packet used to poll a slave. However, it is possible to send packets that cover multiple slots. These multislot packets may be either three or five slots long.

Figure 11
A Bluetooth scatternet.



Scatternet-based PANs

Bluetooth networks will most likely be used to interconnect devices such as cellular phones, PDAs, and notebook computers—in other words, via a PAN. The PAN itself can be a Bluetooth-based IP network—in all likelihood it will be based on a single piconet topology. However, when a PAN user wants to connect to one or more other PANs, Bluetooth scatternet capability will serve as the foundation for the IP network. Similarly, if one or more PANs connect to an Internet access point on a LAN (LAN access point, LAP) a scatternet will provide the underlying Bluetooth infrastructure (Figure 12).

We can expect to see a combination of PAN interconnection and Internet access. In addition, Internet access to one PAN or several interconnected PANs can be provided by using a cellular phone (for example, via GPRS/UMTS) as a bridge/router gateway (Figure 13).[19]

Scatternets can also be rearranged to give better overall performance. For instance, if two slave nodes need to communicate, it might be wiser to create a new piconet that solely contains these two nodes. The nodes can still be part of their original piconets if traffic flows to or from them, or if they need to receive control information. Since the frequency-hopping spread-spectrum (FHSS)

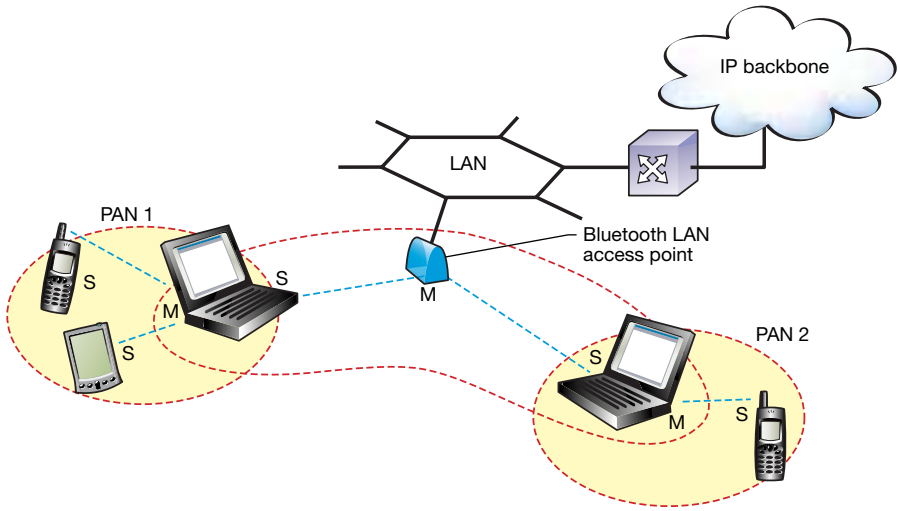


Figure 12
A scatternet with three interconnected piconets, in which two are PANs and one is used to provide network access to the two PANs via a Bluetooth LAN access point. In this scenario, the letters *M* and *S* indicate the distribution of master and slave units.

system makes Bluetooth very robust against interference, new piconets gain substantially more capacity than they lose as a result of increased interference between them.

Scatternet functionality

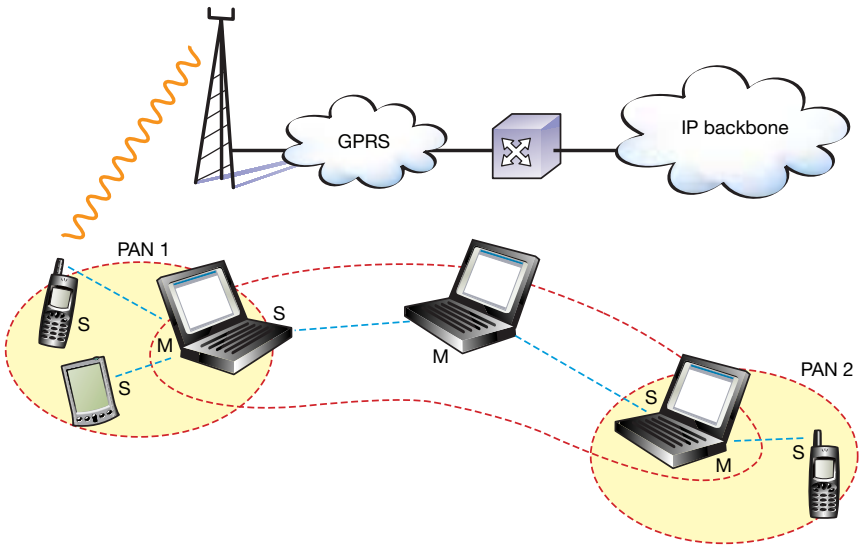
The concept of scatternets offers a flexible way of creating Bluetooth networks and introduces a number of Bluetooth-specific functions. Ideally, these functions should be kept in the background to keep them from bothering the user of the Bluetooth network and to facilitate applications development. The Bluetooth networking functions fall into three main areas:

- scatternet forming and maintenance;
- scatternet-wide packet forwarding; and
- intra- and interpiconet scheduling.

Scatternet forming

To have an efficient infrastructure for IP networking on Bluetooth, piconets and scatternets must be able to adapt to the connectivity, traffic distribution, and node mobility in the network. This is mainly achieved by setting up new piconets or terminating others, in order to attain the optimal scatternet topology. In this context, optimal refers to a scatternet that, for instance, yields minimum delay or maximum throughput.

Figure 13
A scatternet with three interconnected piconets. Via a GPRS/UMTS cellular phone, one piconet provides IP network access to the other two piconets.



But it could also mean minimizing energy consumption in network nodes. To ensure ad hoc operation, the function for forming and maintaining scatternets must be distributed.

Packet forwarding in the scatternet

Forwarding—or routing—becomes necessary when packets must traverse multiple hops between the source and destination nodes. Given that IP will be commonplace in scatternet contexts, one might conclude that routing over the scatternet should be handled within the IP layer (Figure 14). However, there are good arguments for taking another course.

- The current IP dynamic host configuration protocols[20] (DHCP) and emerging zero-configuration methods[21,22] (IETF Zero Configuration Networking Working Group, zeroconfig) rely on link layer connectivity. These protocols are typically used to attain a dynamic IP address for an IP host or to select a random IP address. Generally, the protocols will not work beyond an IP router, which means that they will not reach nodes located more than one Bluetooth hop away in an IP-routed scatternet. A scatternet that provides broadcast segment-like connectivity would enable these protocols to work for Bluetooth-based IP hosts that are separated by multiple hops.
- To operate efficiently, the routing function should be joined with the function for forming scatternets. A routing function on the IP layer would thus need to be adapted to, or interact very closely with, the underlying Bluetooth layer, which violates the idea of keeping the IP layer independent of the link layer technology.
- IP routing is typically performed between networks with different link layer technologies or to separate different network domains. Scatternets use only one technology—Bluetooth—and typically belong to only one network domain.

In summary, the best way of providing networking in a Bluetooth scatternet is to perform the routing on a network layer residing below IP (Figure 15). This layer will

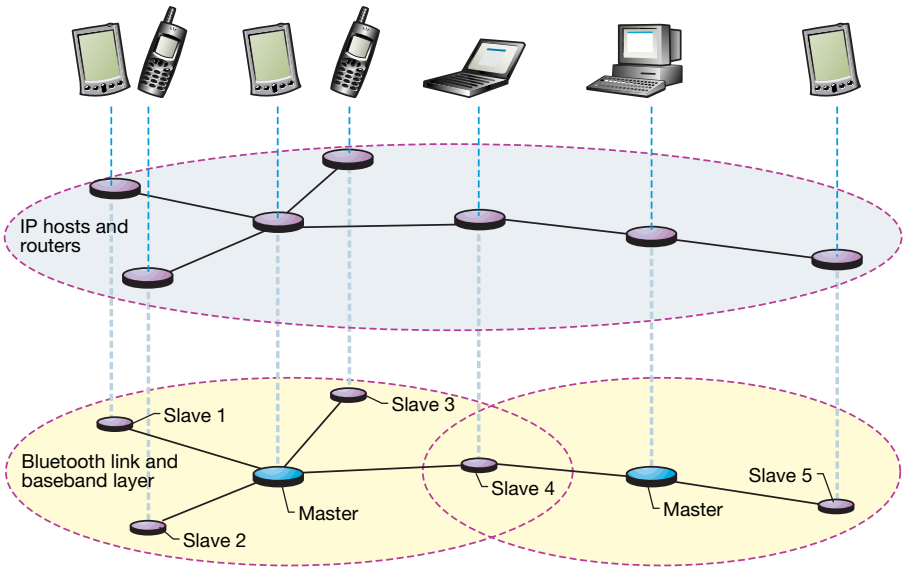
- be able to interact closely with the Bluetooth baseband functions during the establishment or tear-down of a Bluetooth-specific piconet; and
- provide a broadcast segment-like interface to IP.

Intra- and interpiconet scheduling

The master unit of a piconet controls the traffic within the piconet by means of polling. A polling algorithm determines how bandwidth capacity is to be distributed among the slave units. The polling algorithm assesses the capacity needs of the units in the scatternet and ensures that capacity is shared fairly, or according to a weighted capacity-sharing policy.

In a scatternet, at least one Bluetooth unit is member of more than one piconet. These

Figure 14
A Bluetooth scatternet where the networking functionality is handled within the IP layer (that is, by IP routing).



interpiconet nodes might have a slave role in numerous piconets but can have the master role in only one of them. The main challenge is to schedule the presence of the interpiconet node in its different piconets, in order to facilitate the traffic flow both within and between piconets. Given that the interpiconet node is a single transceiver unit, only one of its entities (master or slaves) can be active at a time.

To manage scatternet traffic efficiently, the intrapiconet scheduler must consider the interpiconet scheduler when it polls the slaves of a piconet. For instance, the intrapiconet scheduler in a master unit might not schedule an interpiconet node when the latter is active in another piconet. However, the interpiconet scheduler might schedule this node more often, after it is once again active in the piconet.

The Bluetooth SIG

The Bluetooth Special Interest Group (SIG), comprised of leaders in the telecommunications, computing, and network industries, drives the development of Bluetooth technology and its exposure in the market. The Bluetooth SIG includes promoter companies (3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia and Toshiba) and more than 2000 other companies that have adopted Bluetooth.

The work of specifying the next step in the development of Bluetooth technology has been delegated to a set of working groups. Among them, the Personal Area Networking Working Group (PAN WG) is responsible for developing functions and protocols that will allow IP-based applications to be implemented in Bluetooth devices. The current support provided for IP in the Bluetooth specification needs to be enhanced to facilitate future IP applications—in order to facilitate improved performance and functionality.

Other *ad hoc* technologies

IEEE 802.11

The IEEE 802.11 specification[23] is a wireless LAN standard that specifies a wireless interface between a client and a base station or access point, as well as between wireless clients.

IEEE 802.11 defines two physical characteristics for radio-based wireless local area networks: direct-sequence spread spectrum (DSSS), and frequency-hopping spread spectrum (FHSS), both of which operate on the 2.4 GHz ISM band.

Two network architecture modes have been defined in the IEEE 802.11 standard, namely the point coordination function (PCF) mode and the distributed coordination function (DCF) mode. The former uses a centralized approach in which a network access point controls all traffic in the network, including local traffic between wireless clients in the network. The DCF mode supports direct communication between wireless clients.

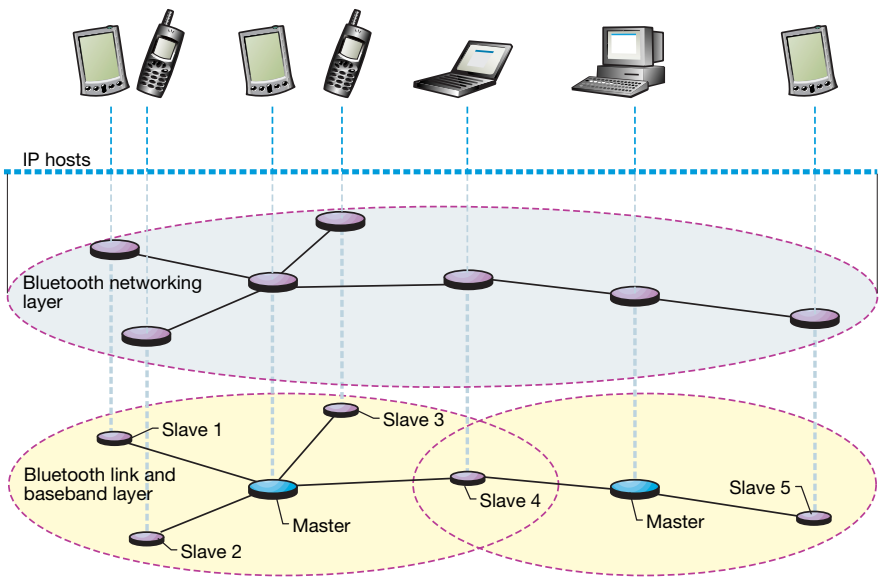


Figure 15
A Bluetooth scatternet where networking is handled within a Bluetooth networking layer, which provides a broadcast segment to the IP hosts.

The media access control (MAC) layer uses the carrier-sense multiple-access-with-collision-avoidance (CSMA/CA) algorithm. A terminal operating in DCF mode that wants to send data: listens to make certain the channel is free and then waits for a randomly drawn period (backoff). If no other station attempts to gain access after this period of waiting, the terminal can gain access according to one of two modes:

- Four-way handshake—the sending node sends a request-to-send (RTS) packet to the receiving terminal. If the receiver accepts the request, it replies with a clear-to-send (CTS) packet. If no collisions have occurred, the sender then begins transmitting its data.
- The sender immediately begins sending its data. This mode is used when the data packet is short.

In either mode, the receiver responds with an acknowledgement (ACK) packet if the packet was successfully received. The CSMA/CA mechanism is also active for the PCF mode. However, because the access point has greater priority than terminals, it has total control of the channel.

The IEEE 802.11 standard does not specify a method for multihop *ad hoc* networking. However, in several experimental networks, MANET-based IP routing has been used. Nonetheless, the experiments did not employ automated host configuring—that is, static IP addresses were assumed.

HiperLAN/2

As a rule, a HiperLAN/2 (H2) network has a centralized mode (CM) in which mobile terminals communicate with access points (AP) over the air interface as defined by the HiperLAN/2 standard. The user of a mobile terminal can move around freely in the HiperLAN/2 network, which ensures that the terminal, and hence, the user, gets the best possible transmission performance.

The development of a high-speed transmission environment with controlled QoS has been the main focus regarding the design choices for the H2 network. The rate of the H2 network will give up to 54 Mbit/s on layer 3 and it will operate in the 5 GHz frequency band.

The connection-oriented nature of H2 makes it easy to implement support for QoS. Each connection can be assigned a specific QoS, for instance in terms of bandwidth, delay, and bit error rate. It is also possible to use a more simple approach, in which each connection can be assigned a priority level relative to other connections. This type of QoS support combined with high transmission rate will facilitate simultaneous transmission of many different types of data stream, such as video and voice.

H2 also provides a direct mode (DM) of communication between mobile terminals, which means that it has some of the properties that fit into the *ad hoc* network category. However, the AP needs to control communication between mobile terminals even though the radio link is direct between the nodes. Thus, any two given H2 mobile terminals cannot communicate on an *ad hoc* basis without having an access point within reach. This differs from the IEEE 802.11 way of managing *ad hoc* communication. Nevertheless, the *ad hoc* mode of operation of H2 is still in its early phase of development and the final design might deviate from this description.[24]

Conclusion

In this article we have tried to survey *ad hoc* networking mainly from a technical point of view. We have also made an attempt to clarify what an *ad hoc* network actually is and found that the definitions vary. However, by proceeding from familiar wireless network architectures, we have allowed the level of independent operation of the network nodes to define the notion of *ad hoc* networking. Typically, these networks operate with distributed functions and allow traffic to pass over multiple radio hops between source and destination.

Furthermore, we have discussed some of the typical properties of *ad hoc* networks, such as routing algorithms and the implications of radio layers. The inherent unpredictability in a network whose nodes move poses a challenge to routing and mobility functions if they are to deliver data consistently between the network nodes. Nonetheless, multihop radio systems also make it possible to save battery capacity while retaining, or even improving, performance. In any case, the most attractive property of an *ad hoc* networking model is perhaps its independence from centralized control and, thus, the increased freedom and flexibility it gives the user.

Ad hoc networks have mostly been used in the military sector, where being able to establish *ad hoc* communication is often a necessity. On the other hand, in the commercial sector, successful examples of *ad hoc* radio networks are few so far, if any. How-

ever, instead of looking at large-scale networks we turned to the small-scale personal area networks that are emerging in response to the introduction of short-range radio technologies, such as Bluetooth. Here, ease of use and flexibility are fueling the demand for *ad hoc* operation. In addition, a centralized network architecture would have serious problems trying to control all PAN devices. In particular, *ad hoc* Bluetooth networks—scatternets—will give rise to a whole new set of business and consumer applications for small, battery-driven user devices, such as mobile phones, PDAs, and notebook computers. The combination of wide-area IP connectivity via UMTS (mobile phone) access, and personal area connectivity in the PAN presents new opportunities for the user on the go. End-to-end IP networking is a key component in this respect, providing the basis on which to develop applications for PAN products. Thus, the current development of IP support in Bluetooth networks is crucial.

Due to its inherent flexibility, *ad hoc* networking is easy to deploy and would fit nicely into, say, an office setting, where users could set up *ad hoc* networking groups using fewer LAN access points and potentially less transmitting power. However, the products that apply the concepts of *ad hoc* networking will most likely see its light in the short, personal area range. These products will mainly focus on facilitating communication between a user's personal devices—either for local traffic or as gateways to the Internet. The *ad hoc* network functionality will also enable the interconnection of different users' devices—for instance, to facilitate larger *ad hoc* working groups. The intrinsic ability to create generic, small-scale, *ad hoc* networks in portable devices represents an entirely new area for future *ad hoc*-based applications.

REFERENCES

1 N. Abramsson "The ALOHA system—another alternative for computer communications" in AFIPS Conf. Proc., vol 37, FJCC, 1970, pp. 695-702.

2 J.Jubin and J.D.Tornow, "The DARPA packet radio network protocol," Proc. Of the IEEE, vol 75, No.1, Jan 1987, pp.21-32.

3 Y.D.Lin and Y.C.Hsu, "Multihop Cellular: A new architecture for wireless communications" in IEEE INFOCOM 2000, pp. 1273-1282.

4 Mobile *Ad hoc* Networks (MANET). URL: http://www.ietf.org/html.charters/manet-charter.html. (2000-05-28). Work in progress.

5 "What's Behind Ricochet: A Network Overview," http://www.ricochet.net/ricochet_advantage/tech_overview.

6 D.C.Steere et. al., "Research challenges in environmental observation and forecasting systems," MOBICOM 2000, pp. 292-299.

7 Christian Gehrmann, Pekka Nikander, "Securing *ad hoc* services, a Jini view," MobiHoc '00, August 2000.

8 Per Johansson, Tony Larsson, Nicklas Hedman, Bartosz Mielczarek, and Mikael Degermark. Scenario-based Performance Analysis of Routing Protocols for Mobile *Ad hoc* Networks. In Proceedings of the Fifth Annual International Conference on Mobile Computing and Networking, August 1999.

9 Charles E. Perkins, "*Ad Hoc* On Demand Distance Vector (AODV) Routing." Internet draft, draft-ietf-manet-aodv-02.txt, November 1998. Work in progress.

10 Josh Broch, David B. Johnsson, David A. Maltz, "The Dynamic Source Routing Protocol for Mobile *Ad hoc* networks." Internet Draft, draft-ietf-manet-dsr-00.txt, March 1998. Work in progress.

11 Charles E. Perkins and Pravin Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers." In Proceedings of the SIGCOM '94 Conference on Communications Architecture, protocols and Applications, pages 234-244, August 1994. A revised version of the paper is available from http://www.cs.umd.edu/projects/mcml/papers/Sigcomm94.ps. (1998-11-29)

12 Charles E. Perkins. RFC 2002: IP Mobility Support, October 1996. Updated by RFC2290. Status: PROPOSED STANDARD.

13 Charles E. Perkins. Mobile IP. IEEE Communications Magazine, pages 84–99, May 1997.

14 Ulf Jönsson, Fredrik Alriksson, Tony Larsson, Per Johansson, Gerald Q. Maguire Jr., "MIPMANET - Mobile IP for Mobile *Ad hoc* Networks," MobiHoc '00, August 2000.

15 L.Kleinrock, and J.Silvester, "Spatial reuse in multihop packet radio nework" Proc. Of the IEEE, vol 75, No.1. pp. 156-166, Jan 87.

16 Haartsen, J.: Bluetooth - The universal radio interface for *ad hoc*, wireless connectivity. Ericsson Review Vol. 75(1998):3, pp. 110-117.

17 J. Hartsen, M. Naghshineh, J. Inouye, O. J. Joeressen and W. Allen, "Bluetooth: Visions, goals, and architecture," ACM Mobile Computing and Communications Review, pp. 38-45, No. 2, Vol. 4, 1998.

18 Bluetooth Specification, Baseband Specification,http://www.bluetooth.com/link/spec/bluetooth_b.pdf

19 Per Johansson et al. Short-Range Radio-Based *Ad hoc* Networking: Performance and Properties ICC'99, Vancouver, 1999

20 R. Droms, "RFC 2131: Dynamic Host Configuration Protocol," March 1997, available from http://www.ietf.org/rfc/rfc2131.txt

21 IETF, Charter of the Zero Configuration Networking (zeroconf) WG, Available from http://www.ietf.org/html.charters/zeroconf-charter.html.

22 S. Cheshire, "Dynamic Configuration of IPv4 link-local addresses," Internet Draft, 8th October 2000, Available from http://www.ietf.org/internet-drafts/draft-ietf-zeroconf-ipv4-linklocal-00.txt

23 IEEE Computer Society LAN MAN Standards Committee, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-1997. The Institute of Electrical and Electronics Engineers, New York.

24 Khun-Jush, J., Malmgren, G., Schramm, P. and Torsner, J.: HIPERLAN type 2 for broadband wireless communication. Ericsson Review Vol. 77(2000):2, pp.108-119.