International Journal of Computer Science and Applications, Vol. 5, No. 4, pp 26 - 44, 2008

A SECURE GATEWAY SOLUTION FOR WIRELESS AD-HOC NETWORKS

SANDIP VIJAY

Computer & Electronics Discipline, DPT, Indian Institute of Technology, Roorkee, Saharanpur Campus, Saharanpur, UP-247001, INDIA
snvijdpt@iitr.ernet.in
http://www.iitr.ernet.in

S. C. SHARMA

Associate Professor, Computer & Electronics Discipline, DPT, Indian Institute of Technology, Roorkee, Saharanpur Campus, Saharanpur, UP-247001, INDIA
subhash1960@rediffmail.com
http://www.iitr.ernet.in

This paper reviewed the secure characteristics of mobile devices that can use wireless networks almost anywhere and anytime by using one or more wireless network technologies. These technologies enable the use of infrastructured networks and ad-hoc networks. Further it describes the characteristics of wireless ad-hoc networks and the environment for the different possible gateway implementation. The gateway implementation provides a secure generic solution for accessing the infrastructured network from the ad-hoc network, and it provides multiple security levels that enable different security levels for different networking environments. It describes the environment in which the gateway is used, introduces potential gateway solutions, and chooses the most appropriate gateway solution and provides the gateway specification for the wireless ad hoc network. The minimum, essential and additional functional requirements are chosen for effective functionality of gateway. At the end, optional functional requirements are not implemented, but they are described with their features that may be implemented in the future.

Keywords: The Gateway; Internet Protocol (IP); 3GPP; Ad-Hoc Network Layers.

1. Introduction to Wireless Ad-Hoc Networks

An ad-hoc network is a collection of wireless nodes that can communicate with each other without any dependence on a fixed infrastructure or centralized administration. Nodes within transmission range can communicate directly with each other, but those out of range must rely on other nodes to forward along packets to their final destination. Because they can be deployed quickly and require no extra planning, ad-hoc networks are often useful for establishing temporary work- groups in war-room settings, single building business meetings, or disaster relief situations.

Isolated wireless ad-hoc networks are not suitable for today's applications that require accessing services in the Internet. To overcome this limitation, one or more devices in the wireless ad-hoc network can provide a gateway to an external network. This external network can be the Internet or a local area network (LAN), which may or may not be an infrastructured network. Wireless networks are more vulnerable to misuse than wired networks. In a wireless network, all devices share the same radio band. If two or more devices transmit simultaneously, the communication fails. In addition, a malicious device may be present in the network. It can analyze the communication in the network and do several attacks by sending invalid data [3]. Several security mechanisms partially protect communication in WLAN. WLAN may provide security on the lower layers that corresponds the physical and link layers of the Open Systems Interconnection (OSI) reference model [31]. These mechanisms protect communication authenticity, integrity and confidentiality by using cryptographic methods. Moreover, these mechanisms depend on the WLAN technology. It is impossible to prevent a malicious device from interfering the transmission in a wireless ad-hoc network [4]. It is also possible that not all devices

can communicate directly in the wireless ad-hoc network. Such a scenario is shown in Fig.1 in which device B can communicate with devices A and C directly, but devices A and C cannot communicate directly. This has an impact on the network-layer and application-layer protocols. In the network-layer, not all devices can communicate directly with each other by using IP addresses. Moreover, some applications do not work unless the communication is link-local. For example, Dynamic Configuration of IPv4 Link-Local Addresses [12] requires link-local communication to successfully configure and maintain IPv4 addresses.

Routing enables communication between devices that cannot communicate directly. In the ad-hoc network, using an ad-hoc routing protocol does this. There are two types of routing protocols for ad-hoc networks: Proactive and Reactive. In proactive routing, routes are actively maintained, and they are available when needed. In reactive routing, routes are discovered on demand. An ad-hoc network can be isolated, or it can have a gateway that provides a connection to another network. Consequently, the devices must be able to communicate when the gateway is available and when it unavailable.

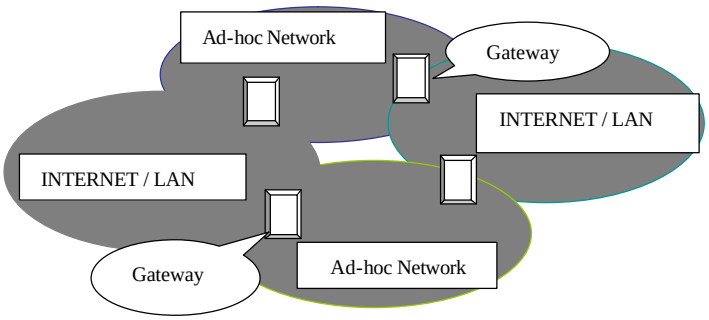

Fig. 1. Communication link between different networks using gateway

2. The Ad-Hoc Network Environment

This section introduces the gateway and its environment, and it describes the used ad-hoc network environment first from the lowest layer upward and then from the logical point of view. The users use wireless devices to communicate with other users in proximity. The devices use Wireless Local Area Network (WLAN) to form a wireless ad-hoc network. The devices can be desktops, laptops, and mobile phones. The communication takes place within a group of two or more people. The communication group may be formed for one communication session only or for many communication sessions. The communication group may remain unchanged during the communication, or it may change constantly. The communication can be personal, professional, or between unknown people. Friends and relatives can use the devices for personal communication. Company employees can use them to organize a project meeting. The users can also use them to communicate temporarily with unknown people.

The users may also need to use services that are not available in the wireless ad-hoc network. They may need to browse web pages, send and receive email, and communicate with other users that are not present in the wireless ad-hoc network. These services are available in infrastructured networks, such as in the Internet or in intranets. A user usually communicates with the infrastructured network through an

access network, e.g. through a cellular network. However, this option is available only to the customers of the operator that provides the access network.

WLAN Technology: WLAN is based on the IEEE 802.11 standard [26] that defines a family of WLAN standards. More specifically, it is based on the 802.11b standard [27] that enables the data transfer rate of 11 Mbps making the performance comparable to that of a wired LAN. In addition, the ad-hoc network is implemented by using the Independent Basic Service Set (IBSS) type of network. This allows devices within range communicate only directly. However, devices must use the same physical channel to communicate, and they must use choose to use the same ad-hoc network because the standard allows coexistence of many networks in the same physical channel. Although WLAN implements the functionality of the physical layer and the link layer, to enable the use of network-layer addresses in the current link, the network-layer addresses must be mapped into Ethernet addresses by using An Ethernet Address Resolution Protocol (ARP) [28] or Neighbor Discovery (ND) [29].

Network Layer: In the network layer, the communication is based on IP. More specifically, either IPv4 [51] or IPv6 [17] is used. It is also possible to use a dual stack in which both IPv4 and IPv6 are used. Also Internet Control Message Protocol (ICMP) [50] is used along with IPv4 for various purposes, e.g. testing the reach ability of a host. Similarly, ICMPv6 [14] is used along with IPv6.

Transport Layer and Session Layer: The Internet Protocol provide unreliable packet delivery of upper level protocols. The User Datagram Protocol (UDP) [29] enables connectionless delivery of application data. The Transmission Control Protocol (TCP) [2] enables connection-oriented communication.

IP can also be encapsulated inside other protocols. When IPsec is used, IP can be encapsulated by using Authentication Header (AH) [30] or IP Internet Key Exchange (IKE) [22]. Moreover, IP can be encapsulated by using IP Encapsulation within IP [5] and Generic Routing Encapsulation (GRE) [19].

Presentation Layer and Application Layer: Using the network requires several services that are provided in the application layer. These services are service discovery service, address configuration, and domain name service (DNS). The service discovery service allows gateway clients to discover the gateway. The address configuration service allows clients to negotiate unique IP addresses. DNS is used to resolve host names and IP addresses in the external network. The next sections describe first services and then logical network structures.

Devices: This work considers devices that are laptops with a WLAN interface, and the operating system used is Linux. In addition, using mobile devices based on the Symbian operating system is an optional solution that is considered here.

A gateway can also provide access to an infrastructured network. A gateway can be either wired or wireless. A wired gateway is usually based on Ethernet (described in [29]) but other technologies can also be used. A wireless gateway can offer network access, for example, by using 3G or WLAN.

Network Structure: In the wireless ad-hoc network, the communication is restricted to the linklocal communication, but the gateway is used enable communication between the wireless ad-hoc network and the infrastructured network. The communication works properly only if all the devices are within each other's communication range. The gateway may also be able to provide globally routable addresses to the gateway clients.

3. Secure Characteristics of Gateway Solutions

In this section, we describe the potential gateway solutions, compare them, and select the most suitable solution for the environment described above.

3GPP System and WLAN Interworking: The 3GPP System and WLAN Interworking specification [2] allows 3G devices to use WLAN as a radio access technology. The specification describes Authentication, Authorization, and Accounting (AAA) through the 3GPP system, the use of an infrastructured network through a WLAN, and Packet Switched (PS) services through a Public Land Mobile Network (PLMN).

Fig. 2 presents the trust model entities in the 3GPP System and WLAN interworking: user, WLAN access provider, and cellular operator. The user uses the 3G functionality of the cellular operator through the WLAN access provider. The WLAN access provider offers WLAN connectivity to the user and an access network to the cellular operator. The WLAN access provider can also be a part of the cellular operator. The cellular operator provides 3G services to the user through the WLAN access provider. The user-operator trust relation (U-O) is based on a legal agreement between the user and the cellular operator. The operator-WLAN trust relation (O-W) is based on roaming agreements or other agreements, or it is internal to the cellular operator if the WLAN access provider is part of the cellular operator. Finally, the user-WLAN trust relation (U-W) is derived from U-O and O-W. Next, we describe the 3GPP system and WLAN interworking architecture in more detail and explain how it is modified to provide a gateway implementation for the environment described above.

Architecture: Fig.3 presents the simplified architecture. A user can access an infrastructured network directly through WLAN or through a Packet Data Gateway (PDG). This requires that the user is successfully authenticated and authorized for access by using the 3GPP AAA server. The 3GPP system and WLAN interworking provides two reference models: the non-roaming and the roaming reference model. In the non-roaming model, a user uses WLAN connected to the 3GPP home network. In contrast, in the roaming model, a user uses WLAN connected to the 3GPP visited network. Here, a user can access the PDG either in the 3GPP home network or in the 3GPP visited network.

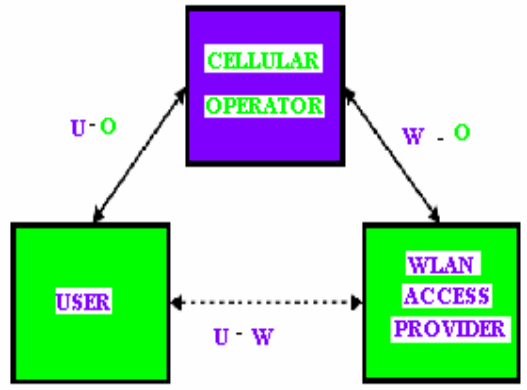

Fig.2 The trust model in 3GPP system and WLAN interworking

Authentication, Authorization, and Accounting: Using 3GPP system and WLAN interworking requires that the cellular operator trusts the WLAN access provider. The cellular operator must allow the WLAN access provider to use its AAA server to authenticate and authorize the users. This also allows the WLAN access provider to generate accounting information that can be used for billing and other purposes. A WLAN access point (AP) uses the AAA information in the AAA server of the 3GPP home network by using an AAA protocol. Both RADIUS [54] and DIAMETER [11] can be used to transport the AAA information over IP.

Authentication is based on the Extensible Authentication Protocol (EAP) [3] that supports multiple authentication methods. Authentication is done by using a

Universal Subscriber Identity Module (USIM) (described in [6]) or by using a Subscriber Identity Module (SIM) (described in [23]). Using EAP between a 3G device and an AAA server is shown in Fig.2. The authentication information is transported between a device and an AAA server. Between a device and AP, EAP is transported over a WLAN protocol. In a 802.11 WLAN, the EAP Over LANs (EAPOL) (described in [28]) is used.

Further, between AP and an AAA server, EAP transported over an AAA protocol. In addition, there can be proxies between AP and the AAA server. The AAA proxy is responsible for obtaining the AAA information from the appropriate AAA proxy or server. Proxies can participate in authorization by further restricting access, and they can store accounting information.

Communication Integrity and Confidentiality: In 802.11 WLAN, link-layer communication integrity and confidentiality are based on the IEEE 802.11i specification [30]. This specification enhances WLAN security by introducing the use of Advanced Encryption Standard (AES) [13]. However, according to the Wi-Fi Alliance's white paper [63], old IEEE 802.11 hardware may not be able to support it.

In the network layer, communication integrity and confidentiality between WLAN and PDG can be provided by using IPsec [60]. Using IPsec is described in [1], but the mechanism to set up a secure tunnel between WLAN and PDG is not yet finalized. However, it does propose a solution. First, a security association is made by using the Internet Key Exchange (IKEv2) Protocol [31], and PDG is authenticated by using public key cryptography with certificates. Second, a device can be authenticated by using EAP with USIM or SIM. Alternatively, IKEv2 or the older version, IKE is used, and both the device and PDG mutually authenticate each other with certificates.

Using 3GPP System and WLAN Interworking as a Gateway: The modified 3GPP system and WLAN interworking allows a 3G device to provide a gateway service in a wireless ad-hoc network as shown in Fig.5. The 3G device uses its standard 3G functionality for IP connectivity and DNS. It allows the gateway clients to access an infrastructured network by using Network Address Translation (NAT) [17].

It also provides a caching DNS service and advertises the gateway service by using ICMP Router Discovery Messages [16] or Neighbor Discovery. Finally, IPsec provides communication integrity and confidentiality between the gateway and the gateway client.

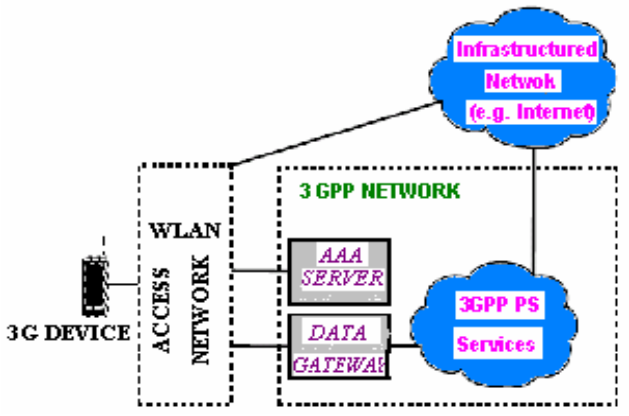

Fig. 3 Simplified 3GPP system and WLAN interworking architecture

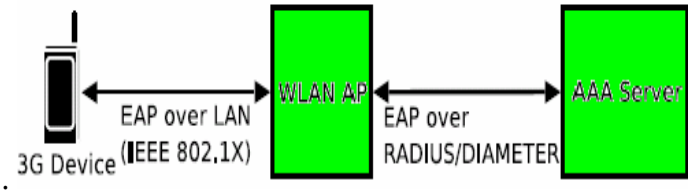

Fig. 4 EAP between a 3G device and an AAA server

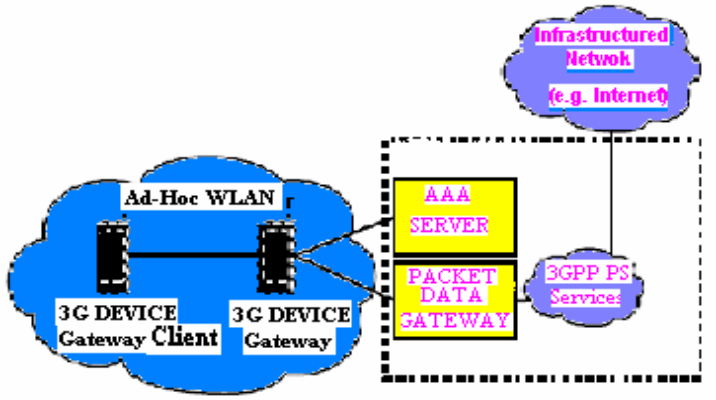

Fig. 5 3 GPP System and WLAN Interworking as a gateway

Authentication, Authorization, and Accounting: As the gateway acts as a client to the cellular operator, the gateway and the cellular operator mutually authenticate and authorize each other by using the standard 3G functionality. The cellular operator also checks that the gateway is authorized to use the AAA server. This allows the gateway and the gateway client to mutually authenticate and authorize each other by using EAP with USIM or SIM as the gateway and the gateway client establish an IPsec tunnel by using IKEv2. The gateway can also further restrict its use by denying access. In addition, the cellular operator stores the total accounting information o f the gateway by using standard 3G functionality. This information represents the total amount of network traffic through the gateway, that is, the traffic caused by the gateway clients the traffic caused by the gateway itself. In addition, the gateway can be allowed to generate accounting information on behalf of the gateway clients. The amount of traffic caused by the gateway is obtained when the amount of client traffic is subtracted from the total amount. However, this requires that the cellular operato r trusts that the gateway generates the accounting information correctly.
Alternatively, the gateway does not generate accounting information, and only the total amount of network traffic through the gateway is available.

Local 3G Radio Link: A 3G device can use its own 3G radio link to access an infrastructured network, and it can use a WLAN interface to access the wireless ad-hoc network. Consequently, the device is a multi-homed host that has a valid IP address in both networks. The device must have routes to both networks, but it does not need to provide routing between the networks. Authentication, authorization, and accounting are based on existing 3G functionality. Each device that needs to access the infrastructured network must mutually authenticate with the cellular operator by using USIM or SIM.

Generic Gateway: A multi-homed device can act as a gateway that enables communication between the wireless ad-hoc network and the infrastructured network

as presented in Fig. 6. As the gateway provides access to an infrastructured network by using NAT, it does not need to configure IP addresses for the gateway clients. IPsec provides Communication integrity and confidentiality between the gateway and the gateway client. The gateway can advertise its availability by using ICMP Router Discovery Messages or Neighbor Discovery. In short, the gateway is just a router. This approach is so generic that it is applicable with any network technology that enables IP based communication.

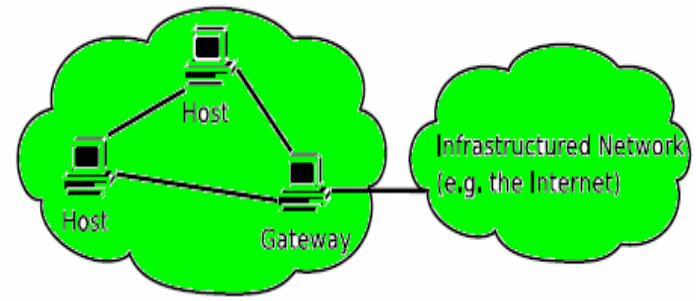

Fig. 6. *Generic Gateway*

Authentication, Authorization, and Accounting: The gateway and the gateway client mutually authenticate and authorize each other as they establish an IPsec tunnel by using IKE with certificates. The AAA information may reside in the gateway or in a remote AAA server. Optionally, the gateway generates accounting information.

Application-Level Gateway: In a wireless ad-hoc network, the gateway can also provide access to an infrastructured network on the application level. The gateway can be a generic proxy for all applications, or it can provide an application-specific proxy for each application.

The gateway can provide a generic SOCKS proxy (described in [21]) that can provide IP connectivity for all applications that support the SOCKS protocol. The SOCKS proxy is shown in Fig. 7. To access an infrastructured network, a gateway client uses the SOCKS protocol to communicate with a SOCKS proxy which in turn communicates in an infrastructured network on behalf of the client. Alternatively, a gateway can provide an application-specific proxy for each application as shown in Fig. 8. This requires that the client can use the protocol through a single proxy only. Here, a gateway client uses an application-specific protocol to communicate with a proxy which in turn communicates in an infrastructured network on behalf of the client. However, using application-specific proxies is possible only with known applications and compatible software versions.

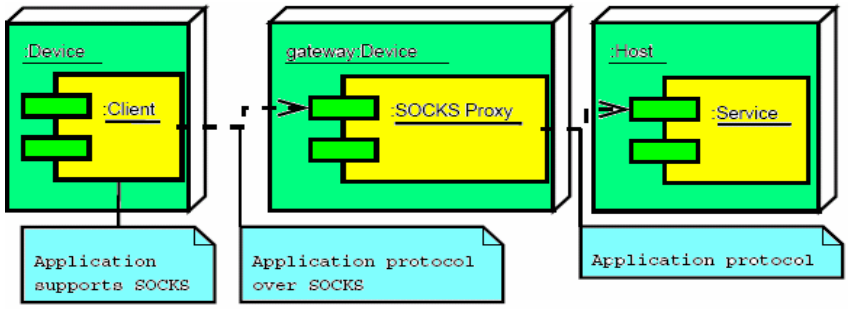

Fig. 7. The generic SOCKS proxy

Optionally, an application-specific proxy is transparent. A transparent proxy is shown in Fig. 9. Using a transparent proxy does not require any modification to a gateway client. Here, a gateway client assumes that it can access an infrastructured network by using the IP address of an infrastructured network as a destination address. The

gateway intercepts the application-specific communication sent by a gateway client, and it acts as a client on behalf of the gateway client in an infrastructured network. It relays the application-specific communication from an infrastructured network to a gateway client as if it came from the infrastructured network.

Authentication, Authorization, and Accounting: Although some applications provide proxy authentication, IPsec can provide authentication and authorization for all applications, and it can also provide communication integrity and confidentiality between the gateway and the gateway client. Optionally, the gateway can also use a remote AAA server. The application-specific proxies do not store traditional accounting information, but they can do application-specific logging that provides application-level information.

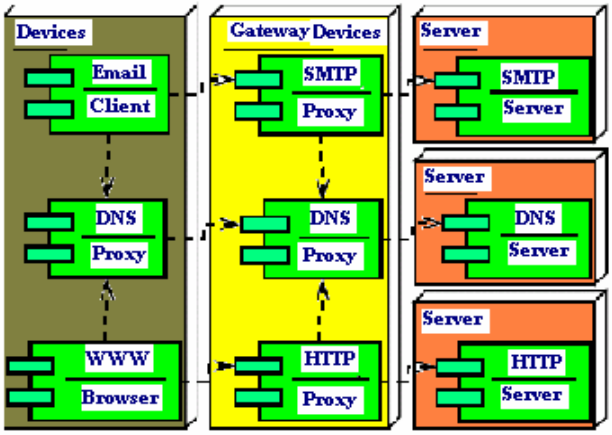

Fig. 8 Application-specific proxies

4. Other Solutions

Striegel, Ramanujan, and Bonney [29] describe a protocol-independent gateway for wireless ad-hoc networks. This gateway can support various ad-hoc routing protocols in the wireless ad-hoc network. The gateway routes traffic between the wireless ad-hoc network and the Internet. It enables Internet access by using either NAT or Mobile IP [46]. However, this solution does not provide any security. Nilsson et. al [11] discuss how IPv6 and Ad-hoc On-Demand Distance Vector Routing (AODV) [17] can be used for Internet access. In this solution, the gateway allocates a globally routable prefix for the ad-hoc network. However, this disables coexistence of multiple gateways because there can be only one global prefix.

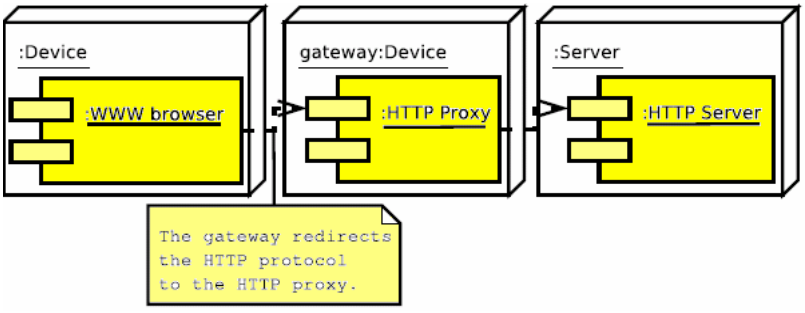

Fig. 9 Transparent proxy

This specification describes a gateway for wireless ad-hoc networks. The business model of the gateway is shown in Fig. 10. The gateway is available only to

authenticate and authorized users, and the users can choose which devices are authenticated and authorized to provide the gateway. The integrity and confidentiality of the gateway communication can be protected in the wireless ad-hoc network. It works with most frequently used applications. It does not require any changes to the external network. Several important choices were made for the gateway implementation. NAT provides a generic solution for accessing external services from the private network, and it works with most frequently used applications. The gateway implementation can provide security for all applications with IPsec. However, using IPsec significantly decreases the performance, and demanding applications may not deliver adequate performance with IPsec. The gateway implementation also provides a DNS service that can resolve host names and addresses in the ad-hoc network and in the infrastructured network without any changes to existing applications. In the gateway business model, there are four roles (Described in Fig. 11): the user, the gateway Fig. 10: The business model of the gateway.

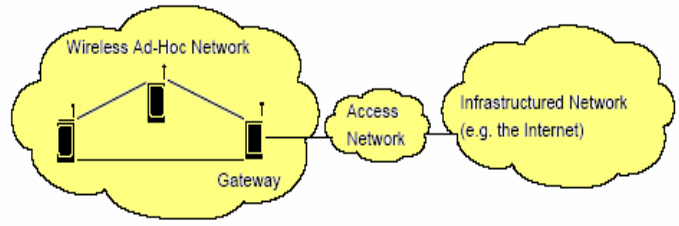

Fig. 10 The business model of the gateway

.

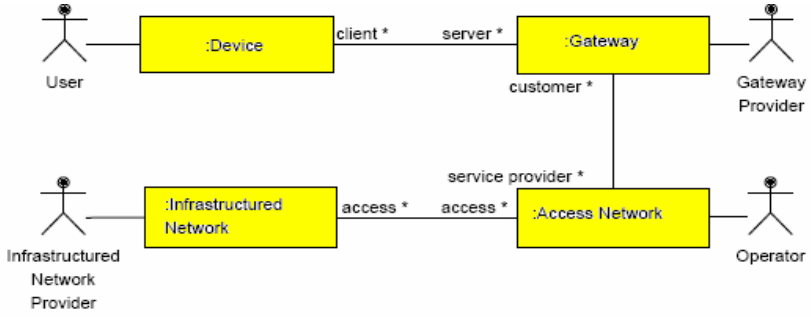

Fig. 11 The roles of gateway business model

The operator provides IP based access to the infrastructured network. The operator may charge a monthly fee or according to the transferred data. In addition, if the gateway provider is visiting a foreign network, the foreign network may charge the roaming costs. The use cases illustrate the basic functionality of the gateway. The use cases are shown in Fig.12. The actors are the users, gateway providers and the operator. The user uses the gateway to access the infrastructured network. The gateway provider provides the gateway to the users. The operator provides access to the infrastructured network.

User a function includes discovers, connect and disconnect. The user discovers the available gateways. The user connects to the gateway. This enables the DNS service and IP based access to the infrastructured network. The user disconnects from the gateway. The user does this explicitly, or this may occur implicitly when the gateway is unavailable.

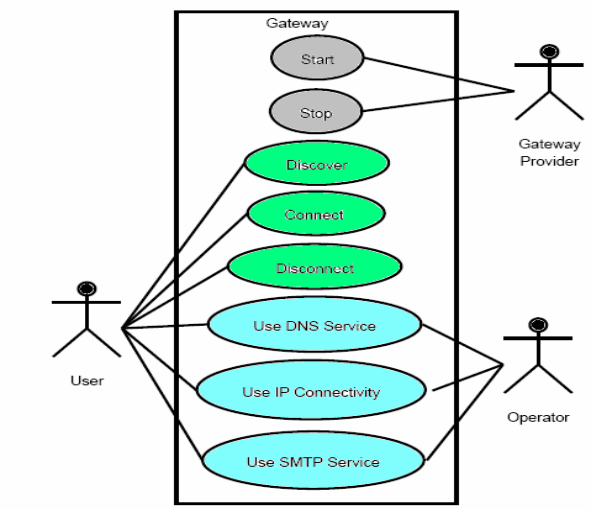

Fig. 12 Use cases for gateway specification

5. Requirements for Gateway specification

There are two types of requirements: functional requirements and nonfunctional requirements. The minimum functional requirements are given in Table 1. There are also additional requirements that extend the usability of the gateway. They do not belong to the minimum requirements; nevertheless, they are mandatory. The additional functional requirements are given in Table 2. The gateway must also conform to the non-functional requirements given in Table 3. Finally, optional functional requirements are not implemented, but they describe features that may be implemented in the future. These requirements are given in Table 4.

Table 1 Functional requirements

ID	Name	Description
A1	Gateway IP Connectivity	The gateway must have IP connectivity to the infrastructured network.
A2	Gateway DNS Service	The gateway must be able to use the DNS service that can resolve host name and addresses in the infrastructured network.
A3	Gateway Discovery	The gateway must be able to allow gateway clients to discover the gateway.
A4	Mutual Authentication and Authorization	The gateway and the gateway client must mutually authenticate and authorized each other before the gateway client use the gateway.
A5	Gateway Configuration	The gateway must provide all necessary configurations for network access to the gateway client.
A6	External IP Connectivity	The gateway must provide the IP connectivity to the infrastructured network for the gateway clients.
A7	External DNS Services	The gateway must provide the DNS services that the gateway clients can use to resolve host names and addresses in the infrastructured networks.
A8	Communication Integrity	The integrity of the communication between the gateway and the gateway client must be protected.

Table 2 Additional functional requirements

ID	Name	Description
B1	SMTP Services	The gateway must provide a SMTP service in the wireless ad-hoc Network.
B2	Multiple Gateways	More than one gateway must be able to coexist in the same wireless ad-hoc networks.

Table 3 Non-functional requirements.

ID	Name	Description
N1	Link-Layer independence	The gateway must be independent of the link-layer technology.

Table 4 Optional functional requirements

ID	Name	Description
X1	Ad-Hoc Routing	The gateway must use an ad-hoc routing protocol and provide access to the infrastructured network through zero or more intermediate nodes.
X2	Routable IP Address	The gateway must provide a routable IP address to the gateway clients. The address must also be routable from the infrastructured network.
X3	Authoritative DNS service	The gateway must provide the DNS service to the infrastructured network that resolves host names and addresses in the wireless ad-hoc network.
X4	Inter-Ad-Hoc Gateway	The gateway must enable IP based access between two or more wireless ad-hoc networks.
X5	Inter Ad-Hoc DNS service	In the wireless ad-hoc network, the gateway must provide the DNS service that resolve host names and addresses in those ad-hoc networks that the gateway provides IP based access too.
X6	IPv4 and IPv6	The gateway must support both IPv4 and IPv6.

6. The Gateway Architecture

The architecture of the gateway is shown in Fig.13. The access network enables communication with the infrastructured network, and it provides services such as DNS and SMTP.

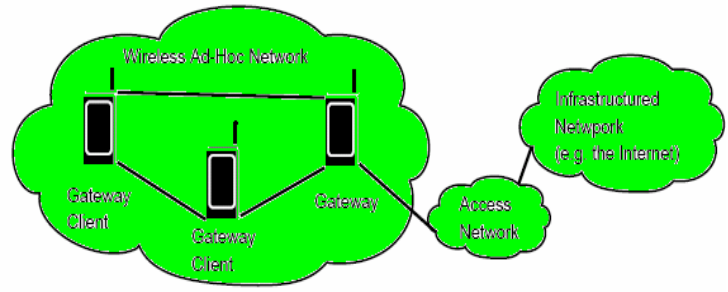

Fig. 13 The Gateway Architecture.

*Wireless Ad-Hoc Network :*In the wireless ad-hoc network, WLAN is based on the IEEE 802.11b standard [7] which enables data transfer rate of 11 Mbps. WLAN is operated in IBSS mode which enables ad-hoc communication without using network infrastructure.

Access Network: The gateway can communicate with the infrastructured network through the access network. Optionally, it provides the SMTP service.

Security: The architecture from the security point of view is shown in Fig.14. To enable optimal settings for different network configurations, the gateway supports the following security levels defined in the SESSI project [6] (Defined in table 5.): (a) None: No security is provided. (b) Authentication: Authentication, authorization, and integrity are provided. (c) Confidentiality: Authentication, authorization, integrity, and Confidentiality are provided. However, the firewall is not a part of the gateway implementation.

7. The Internal Architecture of Gateway

The Internal Architecture describes the architectural components of the gateway. The gateway and the gateway client are similar enough to share the same implementation. This implementation can be started as a gateway or a gateway client. The internal architecture of the gateway implementation is shown in Fig.15. The network interfaces used by the gateway are shown in Fig. 7. The DNS proxy uses the loopback interface to provide DNS locally in the current device.

Table 5 Security levels supported by the gateway.

Services	Authorization	Authentication	Confidentiality
Gateway Discovery	YES	YES	YES
IP Connectivity DNS Services (Infrastructured Network)	YES YES	YES YES	YES YES
DNS Services (Wireless Ad-Hoc network)	YES	NO	NO

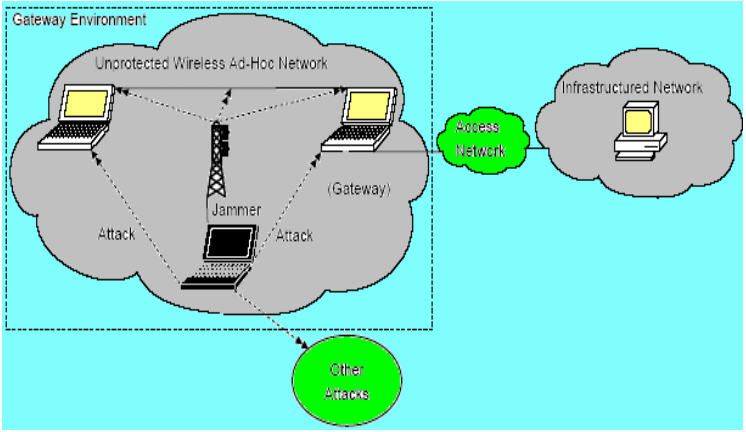

Fig. 14 Security.

Virtual Interface using IPsec in tunnel mode between the gateway and the gateway client creates virtual interfaces that enable communication through the IPsec tunnel. This requires that the tunneled data is communicated by using concrete interfaces such as WLAN interfaces. The WLAN interface enables communication in the wireless ad-hoc network. Therefore, WLAN must support the ad-hoc mode. WLAN is used for link local communication only. It can start gateway component as a gateway or as a gateway client. As a gateway, it provides start the gateway and stop the gateway functions.

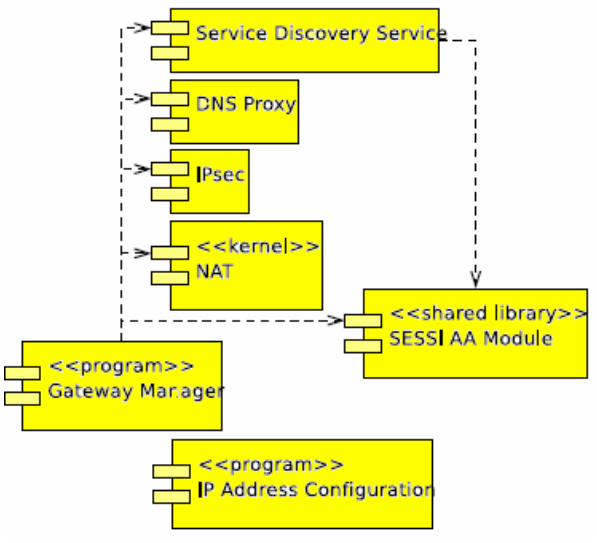

Fig. 15 The internal architecture of the gateway

The external interface allows the gateway to communicate with the infrastructured network. The gateway manager controls the other gateway components. It is a program that provides a command line interface.

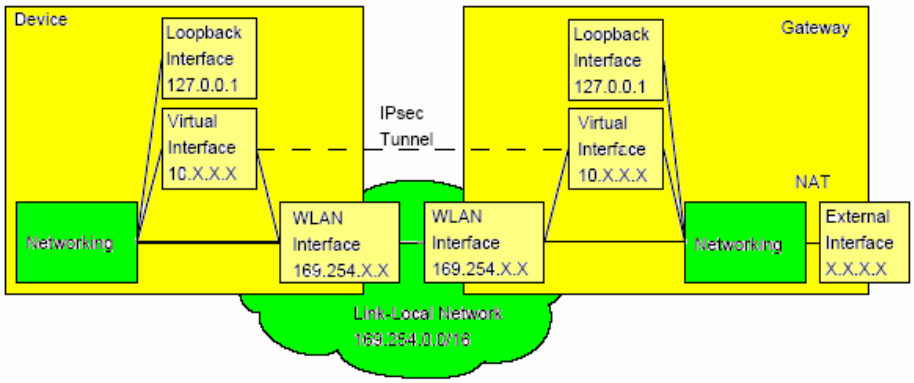

Fig. 16 Network Interfaces

On the other hand, as a gateway client, it provides connect to the gateway and disconnect from the gateway functions. The service discovery service enables gateway discovery in the wireless ad-hoc network. The gateway manager uses the service discovery service for two purposes:

- When the gateway component acts as a gateway, the gateway manager uses the service discovery service to advertise the gateway to the gateway clients.

When the gateway component stops acting as a gateway, it stops advertising the gateway.

• When the gateway component acts as a gateway client, the gateway manager uses the service discovery service to discover available gateways.

The gateway advertises itself by using an SLP URL [21]. The gateway client uses the same URL to discover gateways. The URL is defined as follows: service:gateway.sessi:://IP_ADDRESS. Here, the suffix .sessi defines the naming authority. *Security:*The service discovery service must be able to provide mutual authentication, mutual authorization, communication integrity, and communication confidentiality within the service discovery protocol.

DNS Proxy: The DNS proxy provides a DNS service that can resolve host names and addresses in an infrastructured network and in a wireless ad-hoc network within the link-local scope. The deployment of the DNS proxies is shown in Fig.8. The DNS proxy distinguishes queries between the wireless ad-hoc network and the infrastructured network by applying the following rule:

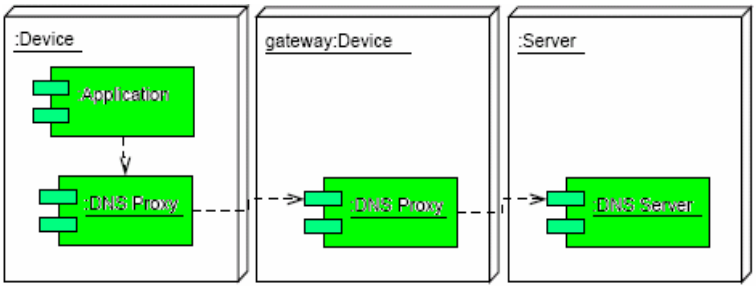

Fig.17. *The deployment of the DNS proxies*

1. The query is resolved locally in the wireless ad-hoc network with mDNS. If either of the following conditions is met:

• The IP address is a link-local address within the range of 169.254.0.0/16.

• The host name ends with the suffix .local.

2. Otherwise, the query is resolved externally with DNS. *Security* : IPsec protects the DNS protocol between the gateway and the gateway client. In addition, when the device boots, the DNS proxy is started along with other networking components. The design of the DNS proxy is given in Fig.17. An application resolves host names and addresses by using the resolver library, which is an integral part of BIND [9]. The DNS proxy can be provided by one of the following implementations: (a) *named*, which is an integral part of BIND (b) pdnsd [5], which is a lightweight DNS server (c) djbdns [4], which is another DNS server

Moreover, the DNS proxy is modified to use mDNS to resolve local host names and addresses in the wireless ad-hoc network. The mDNS implementation is based on Rendezvous [5].

SMTP : The gateway redirects incoming SMTP connections to the external SMTP server by using destination NAT (DNAT) [40].

IPsec :When the gateway acts as a client or a server, it uses IPsec that enables secure communication through the WLAN interface. IPsec can be provided in one of the following ways:

• IPsec is provided by the Linux kernel, KAME tools, and an IKE daemon. [5]

• IPsec is provided by using a FreeS/WAN implementation with X.509 certificate support [5]

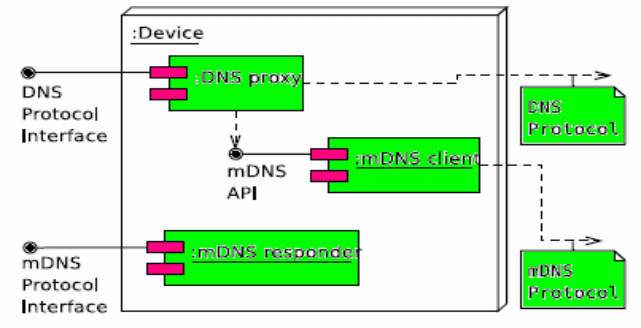

Fig. 18 The design of the DNS proxy

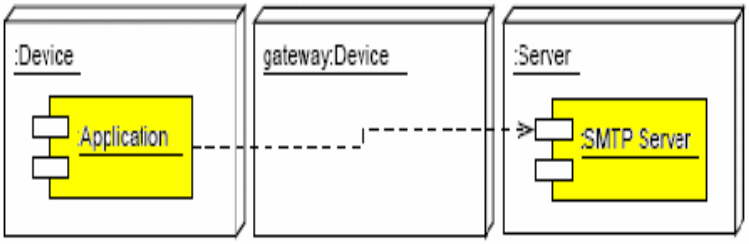

Fig. 19 The deployment of the SMTP server

NAT : NAT is provided by the kernel. It can be enabled by using iptables.
SESSI : Authentication and Authorization Module because the SESSI authentication and authorization module is based on an existing implementation, the design is not included in this document. The SESSI authentication and authorization module is described in detail in the SESSI project documentation [6].

8. Gateway Design Criterion

This section contains the design of the components. It describes how these components are implemented. It also describes which tools and libraries are used.
Gateway Manager : The gateway manager controls the gateway components. The design of the gateway manager is given in Fig.11. Next, the classes of the gateway manager are introduced.
ControlSDS : ControlSDS controls the service discovery service. It provides the following functions:
• discover Gateways: Discover available gateways in the wireless ad-hoc network.
• enable Gateway Discovery: Enable gateway discovery. This allows gateway client to discover the gateway.
• disable Gateway Discovery: Disable gateway discovery. This prevents gateway clients from discovering the gateway.
Control DNS Proxy :This class controls the DNS proxy. It provides the following functions:
• enable Serving DNS: Enable the DNS proxy to use the specified DNS proxies or servers.
Control IPsec :This class controls IPsec. It provides (a) enableIPsecClient: Configure and enable IPsec for the gateway client. (b) enableIPsecServer: Configure and enable IPsec for the gateway. (c) disableIPsec: Disable IPsec for the gateway or the gateway client. Before IPsec is enabled, the following settings must be configuring d for IP address of the gateway and the keys of the gateway and the keys of the

gateway clients. Moreover, if the IP address of the gateway or the gateway client changes, IPsec must be restarted or reconfigure d.

Control NAT: This class controls NAT. It provides enableNAT and disableNAT functions. Where the enableNAT will Enable NAT and disableNAT will Disable NAT.NAT is applied only to the external interface of the gateway by using iptables [4]. As the gateway may have a dynamic IP address for its external interfa ce, NAT can be implemented by using MASQUERADE [4] that drops all network address and port translations if the external IP address changes.

MonitorIPconf : This class monitors IP address configuration. It provides the checkIPChange functions

Check if the IP address has changed. Checking the IP change can be implemented in two alternative ways:

1. The function uses iptables to monitor the messages related to obtaining and claiming an IP address. This allows the gateway manager to take action immediately, but this solution is dependent on the IP address configuration protocol.
2. The function periodically checks the IP address by using the ioctl function available on UNIX platforms. This results in a delay, but this solution is independent of the IP address configuration protocol.

*Service Discovery Service :*Because the service discovery service is based on an existing implementation, the design is not included in this document.

Software development

Design Principles

Simplicity, Minimum Effort, Independence

Operating System

The software is intended to be run on Linux. The kernel version should be as new as possible because some components may require functionality that is unavailable in earlier kernel versions.

Programming Language

The software is written in the C++ language, but it provides a C APIs that can also be used from programs written in C.

Compiler

The gcc C/C++ compiler version 1.1.1 or higher is used.

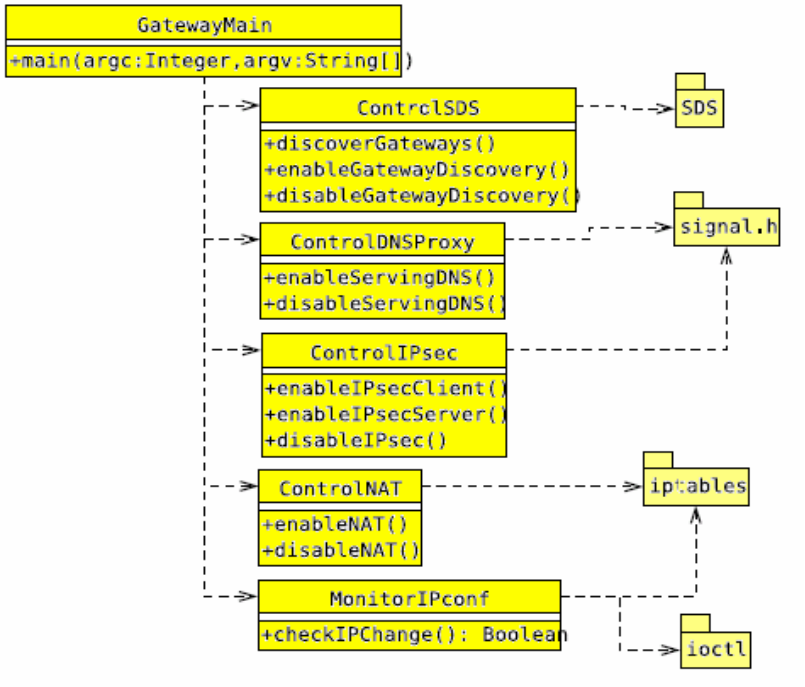

Fig. 20. *The Gateway manager*

9. Conclusions and Future Work

The gateway manager provides a centralized approach for managing changes in the ad-hoc network because it can reconfigure or restart services based on existing implementations. However, building and designing new services from scratch for ad-hoc networks can enable more seamless operation as the services can independently manage changes in the ad-hoc network. Alternatively, static IP addresses can be provided to existing implementations in the network layer. If IP addresses are available, the IP based service discovery service can be used to discover both infrastructural services and application-specific services. Consequently, only one service discovery service is needed. The implemented DNS proxy enables resolving host names and addresses in the wireless ad-hoc network and in the external network without any changes to existing applications. Because the addresses may change in the wireless ad-hoc network, the DNS proxy must use small TTL values or disable caching for local host names and addresses. Alternatively, the DNS proxy must monitor the network and keep the cache up to date. Although IPsec can protect the DNS protocol, it cannot protect the mDNS protocol that uses multicasting. The gateway can also be extended to use private addresses in the wireless ad hoc networks and to use tunnels between the networks. Here, the gateways are used to build a large private network in which NAT is not needed. Also, infrastructured networks with private or global IP addresses can join the private network. Nevertheless, other infrastructured networks are accessed through NAT. Although the gateway implementation only provides half of this functionality, it is one step towards global IP connectivity.

The gateway implementation provides a secure generic solution for accessing the infrastructured network from the ad-hoc network, and it provides multiple security levels for different network environments. It works with most frequently used applications.

Next, the most appropriate gateway solution is chosen from the previously presented gateway solutions according to a brief comparison. A 3G device can use its local 3G

radio link to provide the gateway service to it. When configured correctly, it can directly access both the ad-hoc network and the infrastructured network. However, this option is available to 3G devices only. Moreover, to use the gateway based on 3GPP System and WLAN Interworking, the device must be a 3G device. From the technical point of view, this solution is obsolete because the device does not need to use this solution because it can use its local 3G radio link to provide the gateway service to itself. However, this solution can be meaningful from the business perspective. For example, if the devices are used in a foreign country, one of the devices might have a local USIM or SIM that enables Internet access at a moderate charge. Still, this solution is not very useful under normal circumstances. Although the application-level gateway is independent of the network technology, it depends on the applications. The gateway must support all applications that are used. In addition, when a new application is added, a new proxy must be added. Consequently, as the application-level gateway supports a fixed set of applications only, it lacks generality, and it is not practical for evolving applications. In contrast, the generic gateway is independent of the device type, the network technology, and the applications. Therefore, it is the preferred gateway solution.

References

1. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowetz, H.(2004). Extensible Authentication Protocol (EAP). IETF RFC 3748.
2. Aboba, B., & Dixon, W. (2004) IPsec-Network Address Translation (NAT) Compatibility Requirements. Tech. rep., IETF.
3. Arkko, J., & Haverinen, H.(2004) Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAPAKA). Internet draft, IETF.
4. Arkko, J., Kempf, J., Sommerfeld, B., Zill, B., & Nikander, P. (2004). Secure Neighbor Discovery (SEND). Internet draft, IETF.
5. Bernstein, D. (2004) djbdns: Domain Name System tools. *BIND9.NET. DNS, BIND, DHCP, LDAP* and Directory Services.
6. Buddhikot, M., Hari, A., Singh, K., and Miller, S.(2003). MobileNAT: A New Technique for Mobility across Heterogeneous Address Spaces. In Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots: ACM Press. 75- 84.
7. Calhoun, P., Loughney, J., Guttman, E., Zorn, G., & Arkko, J. (2003). Diameter Base Protocol. RFC RFC3588, IETF.
8. Cheshire, S., Aboba, B., and Guttman, E. (2004). Dynamic Configuration of IPv4 Link-Local Addresses. Internet draft, IETF.
9. Cheshire, S., and Krochmal, M. (2004). Multicast DNS. Internet draft, Apple Computer, Inc. http://files.multicastdns.org/draft-cheshire-dnsext-multicastdns.txt.
10. Conta, A., and Deering, S. (1998). Internet Control Message Protocol (ICMPv6) for the Internet Protocol version 6 (ipv6) specifications. RFC 2463, IETF.
11. Crispin, M. INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1. RFC 2060, IETF, December 1996.
12. Deering, S. ICMP Router Discovery Messages. RFC 1256, IETF, September 1991.
13. Deering, S., and Hinden, R. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, IETF, December 1998.
14. Eastlake, D. Domain Name System Security Extensions. RFC 2535,

15. IETF, March 1999.
16. Farinacci, D., Li, T., Hanks, S., Meyer, D., and Traina, P.Generic Routing Encapsulation (GRE). RFC 2784, IETF, March 2000. Glenn, R., and Kent, S. The NULL Encryption Algorithm and Its Use With IPsec. RFC 2410, IETF, November 1998.
17. Guttman, E., Perkins, C., Veizades, J., and Day, M. Service Location Protocol, Version 2. RFC 2608, IETF, June 1999.
18. Harkins, D., and Carrel, D. The Internet Key Exchange (IKE). RFC 2409, IETF, November 1998.
19. Haverinen, H., and Salowey, J. Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAPSIM) Internet draft, IETF, October 2004. Hertzog, R. Overview of zcip source package. , 2004. Referred: 26 Nov 2004.
20. Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and Stenberg, M. UDP Encapsulation of IPsec ESP Packets. Internet draft, IETF, May 2004.
21. IEEE. IEEE Std 802.11 1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11 1999 ed. IEEE, 1999.
22. IEEE. IEEE Std 802.11b-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer extension in the 2.4 GHz Band, IEEE Std 802.11b-1999 ed. IEEE, 1999.
23. IEEE. IEEE Std 802.1X-2001, Port-Based Network Access Control, IEEE Std 802.1X-2001 ed. IEEE, 2001.
24. IEEE. IEEE Std 802.3-2002, Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, IEEE Std 802.3-2002 ed. IEEE, 2002.
25. IEEE. IEEE Std 802.11i-2004, Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i-2004 ed. IEEE, 2004.
26. ISO. Information technology- Open Systems Interconnection - Basic Reference Model: The Basic Model, ISO/IEC 7498-1:1994 ed., 1994.
27. Kaufman, C. Internet Key Exchange (IKEv2) Protocol. Internet draft, IETF, September 2004. Kent, S., and Atkinson, R. IP Authentication Header. RFC 2402, IETF, November 1998.
28. Kent, S., and Atkinson, R. IP Encapsulating Security Payload (ESP). RFC 2406, IETF, November 1998.
29. Kivinen, T., Huttunen, A., Swander, B., and Volpe, V. Negotiation of NAT-Traversal in the IKE. Internet draft, IETF, February 2004.
30. Klensin, J. Simple Mail Transfer Protocol. RFC 2821, IETF, April 2001.
31. Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D., and Jones, L. SOCKS Protocol Version 5. RFC 1928, IETF.