Heterogeneous Communications Enabled by Cellular Operators

Marc Danzeisen [1][2], Torsten Braun [2], Daniel Rodellar [1], Simon Winiker [1]
[1] Swisscom AG, Innovations, CH-3050 Bern, Switzerland
[2] University of Bern, Computer Networks and Distributed Systems, Bern, Switzerland

Abstract: *How can a secure data communication between two users not knowing each other be achieved? In this paper we show that it is possible to perform such a secured communication using a user friendly setup with help of a cellular network. The main contribution of this paper is to present a secure connection between two users on whatever technology (Wireless LAN, Bluetooth, etc) with an easy installation and setup reusing a cellular network. We describe a novel architecture to enable user friendly establishment of a secure communication among mobile devices to share data using different wireless technologies like wireless LAN, Bluetooth, cellular systems or even infrared. Making use of these technology combinations for data transmission and using the cellular network for signaling, we analyze several scenarios with increasing complexity. The complete picture appears in the last scenario where several heterogeneous technologies are involved and the network is composed of heterogeneous mobile nodes. The novelty of our concept is mainly the usage of Wireless WAN networks to authenticate users and exchange keys to secure the heterogeneous links between the mobile nodes.*

Introduction

Today, mobile wireless networking combines data connectivity with user mobility. Mobile users access their data using technologies like wireless LAN (WLAN) [1], Bluetooth [2], or GPRS [3]. In this paper we consider networking applications enabled by these technologies. We are especially interested in the establishment of Virtual Private Networks (VPNs) among mobile nodes, where a given set of mobile devices use one or several wireless communication technologies to establish a secured common networking area to share their data.

To have a clear view on the issues to be solved, a scenario is proposed as example. Bob has two personal devices for communications, a laptop and a cellular phone. His colleague Alice is carrying three personal devices, a laptop, a cellular phone and her personal digital assistant (PDA). Assume that Bob now wants to send a digital document to Alice. If they are sitting face to face and trust each other, they could exchange the document by simply configuring the interfaces of their devices (for example laptop to laptop). If Alice and Bob are standard users they will need to learn how to configure and connect their devices (we assume that the

 1556-6072/06/$20.00©2006IEEE

THE AD HOC FORM OF WLAN COMMUNICATIONS IS ESPECIALLY USEFUL IN PUBLIC-SAFETY AND SEARCH-AND-RESCUE APPLICATIONS.

drivers, cards and setup are already provided). In the case of heterogeneous networks involved, some devices will be required to play the role of the gateway between technologies. To complete the networking and provide connectivity to the Internet, Internet Connection Sharing (ICS) needs to be enabled on one of the devices. In the simple case where only one technology is present, i.e., WLAN, an SSID has to be exchanged between Alice and Bob, and to make the transfer secure they need to specify WEP settings, but this would probably be the last action to take (because it's easier to get an ad hoc wireless network running smoothly before attempting to configure WEP data encryption) but even in this case there is a security and trust issue as we will see in the next sections. Alice and Bob need to have the same workgroup configured with appropriate permissions for file and printer sharing, and then they can start exchanging the file. Because of this complexity, users prefer to exchange documents using IR technology or external USB memory sticks.

In case Alice and Bob are physically far from each other, or there is no trust relation between them, we propose a service framework to exchange the security and configuration parameters to securely transfer the document in an easy and user friendly way. The service framework can be extended also to the case where Alice and Bob are close to each other, and the service facilitates the transfer of information by helping the users to do all the tedious configurations in an automatic matter. Therefore, Bob sends a service request to Alice's mobile phone, she then may decide to which broadband device the file has to be transferred (laptop or PDA, for example). The selection of the device could also be done automatically depending on a selection of profiles for the incoming information. The proposed system triggers this chosen device to acquire data connectivity (LAN access, WLAN access, Bluetooth access, or any other data access to Internet). Finally, Bob and Alice are able to let their devices start the document transfer.

Every data connection requires a signaling plane to establish the connection, and the framework we propose in this paper is not only a challenge technically but also in terms of pure ad-hoc networking experts' acceptance. Most of the configurations and exchanges can be done without an operator providing this service, but users do not care on the configuration aspects (the less they need to configure the better), and just want to use the services with as less hurdles as possible.

The ad hoc form of WLAN communications is especially useful in public-safety and search-and-rescue applications. Medical teams require fast, effective communications when they rush to a disaster to treat victims. They can't afford the time to run cabling and install networking hardware. The medical team can utilize 802.11 radio NICs in their laptops and PDAs and enable broadband wireless data communications as soon as they arrive on the scene. For these issues, they normally preinstall all devices before starting to use them. With our proposal, the pre-configuration is not required, because the installation is self-made by the devices on site.

The paper is organized as follows: we begin with an introduction explaining the current situation and continue by analyzing the problems users have to face when they want to establish secured communication channels among their mobile devices. After our vision of future heterogeneous networking presentation, the key contribution of this paper is exposed: we propose a concept to use the cellular network to offer authentication and key exchange. The discussion on different case studies makes this proposal more concrete and allows better understanding and positioning of the whole framework for this study. The framework is extended to cope with heterogeneous interconnections between the participating devices. The architectural design is finally discussed and some outlook on future work is given.

Secured Mobile Communications

When users want to establish a secured connection between their mobile nodes, several actions have to be taken. The users have to be aware of the capabilities of their devices and often also require certain knowledge about the communication technologies supported by these devices. For example, in the case of WLAN, different parameters like the operation mode (Infrastructure or Ad-hoc) and the SSID have to be set, before the devices become visible to each other. If the user takes this hurdle, the proper identification and authentication of the correspondent node has to be managed. Assume that Alice wants to transfer a file from her laptop to Bob, who is in the same room using Bluetooth. Even if Alice can see that the person sitting next to him is Bob, she can not be sure that the Bluetooth device her laptop is communicating with is really belonging to Bob and not to somebody else sitting in the very next room. What is needed to resolve this uncertainty is a method to prove that the chosen Bluetooth device is actually belonging to Bob's laptop. The simplest and thus mostly used mechanisms for that are based on shared secrets; the involved mobile nodes have to know a certain value to prove the integrity of their device addresses and their authorization to establish the secured communication. In most of today's situations, this happens either verbally or by writing down the credentials (i.e., the shared key).

After establishing the connectivity among the authenticated nodes, the links have to be secured. Therefore, the nodes have to agree on security parameters. The smallest set of security credentials includes an encryption algorithm and an encryption key. For more sophisticated security measures further information has to be negotiated like the authentication mechanism and the key for authenticating the transmitted data, etc. In other words, there has to be a primary handshake procedure to establish a secure communication link between two or more mobile nodes. This exchange of information must also happen in a secure way.

These parameter negotiations for communication and security form the main part of the signaling needed to establish a secured private connection between mobile nodes. In the case of a self-organizing technology, like Bluetooth, where the nodes are able to discover their neighborhood and automatically establish a communication link, the signaling information is reduced to the authentication process and the exchange of security parameters.

A Vision of Convenient Heterogeneous Wireless Networking

We believe that users do not want to be aware of all these different configuration and security issues; end users just want to securely transfer a file from one of their devices to a certain person. This brings up two main requirements for our vision on heterogeneous wireless networking. First, each user needs his own individual identifier, for instance his mobile subscriber phone number (MSISDN, the number used to call a mobile subscriber). An MSISDN consists of a country code, a national destination code and a subscriber number, and every MSISDN is associated with a Subscriber Identity Module (SIM) card, which the mobile subscriber inserts into the mobile terminal. It contains a code that uniquely identifies an individual subscriber to the network. Additionally, the sender often does not know what type of device the receiver has. Hence, it is up to the receiver to decide which of his devices should be involved in the specific transaction. This abstraction of the destination node to one statically existing personal identifier helps to solve the problem of temporary identifiers of the different destination nodes. Most of nowadays broadband wireless connections are charged based on time and therefore connected on demand having only temporary valid identifiers like leased IP addresses. This restricted reachability can be improved using a signaling plane with high availability that is always on and that uses a traffic based billing scheme, rather than a time based one. So if the sender can reach the receiver by a static, personal identifier, the receiver can trigger the appropriate device to become temporarily connected to the broadband access and fulfill the requested transaction.

The second main requirement to make heterogeneous networking convenient is probably the automatic choice of the most suitable communication technology to cover the needs of a certain service at the lowest possible costs. This is of high importance when the involved nodes are interconnected by the help of access providers.

Authentication and Key Exchange by Cellular Operators

Since the authentication is based on a verification process, the involved entities and mechanisms have to be trusted. Therefore, the question of the underlying trust model is of fundamental importance for the security model. In this paper we distinguish three different trust mechanisms as suggested in [4], [10].

- **Trust by Definition** is the easiest way of trust establishment. Legal authorities, big companies (like banks) and operators are often trusted a priori, or by definition. Such entities have to be reachable for every verification process and referred to as a part of a fixed infrastructure.
- **Trust based on heuristics** is the most natural trust establishment, which happens often in the social life. Entities make the level of trust they have in other entities dependent on their experience with the latter. As this model is based on experience, it can be a very time consuming and hard to deploy approach. Furthermore, the level of security that can be achieved with this trust mechanism is limited. One entity can behave well several times therefore gain a good reputation, but act malicious during the very next transaction.
- **Trust by delegation** is made through third parties, with which a trust relationship already exists. This relation again is based on one of the two trust models, mentioned before. Therefore a trust relation chain has to begin somewhere, with either a trust based on heuristics or with a trust by definition relation. In pure ad-hoc networks [4], [6] where no fixed infrastructure is available, the only possibility to anchor a trust relation chain is the application of the 'Trust by Heuristics' model.

The Cellular Operator as a Signaling and Configuration Provider

Due to the time consuming and unreliable characteristics of the trust by heuristics, trust by definition is the most appropriate model for a platform offering commercial services. Furthermore, in mobile and fixed communication scenarios there is a strong need of signaling channels to establish and manage data communications. For heterogeneous networks we propose a common signaling plane for all the different technologies. This signaling plane must also be always reachable. Therefore, it makes sense to reuse a cellular infrastructure.

WHEN USERS WANT TO ESTABLISH A SECURED CONNECTION BETWEEN THEIR MOBILE NODES, SEVERAL ACTIONS HAVE TO BE TAKEN.

Another approach, where a common signaling plane is used to manage different technologies is introduced by the Multimedia Integrated network by Radio Access Innovation (MIRAI) project [7]. In their proposal the wireless physical layer can be configured dynamically using a programmable radio, referred to as Software Defined Radios (SDR) [8] to provide access to different wireless network technologies offered at the specific location. The common signaling channel called Basic Access Network (BAN) is used to learn about the different access networks that are available and is therefore mandatory for all MIRAI nodes.

In contrast to MIRAI, where the signaling channel is newly designed, we propose to re-use a existing cellular system. A cellular network like GSM meets very well the requirements of such a signaling medium because of its high availability, the built-in security mechanisms and the provided always-on feature. We propose to use the cellular network to provide the signaling and support for an ad-hoc communication, from the setup phase until the end of the data transfer. The large coverage of the cellular system makes it very valuable as a signaling system for wireless broadband connections. The cellular operator will locate the related peers and provide the security mechanisms including the authentication. Furthermore the operator's billing system can be reused to charge the provided authentication service.

To establish a secured link or a Virtual Private Network (VPN) connection between mobile nodes that do not have any prior security relationship with each other, one has to be able to interact with the infrastructure of an operator. For nodes that are connected to a cellular network the required authentication processes are based on the existing cellular mechanisms, i.e., the SIM authentication. Before being able to securely access the cellular network, the node has to successfully manage a challenge/response authentication. The SIM authentication concept also offers a method to derive session keys (KC) to encrypt the communication between the node and the operator's network. Nowadays, the verification of the identity of a user is limited to the ownership of the SIM (i.e., the shared secret Ki) and knowledge of the appropriate PIN to enable that SIM card. However, SIM capabilities are required to interact with the cellular network. This is a very hard constraint since most of today's portable devices, like notebooks or PDAs, do not offer this feature.

This authentication is done by a single node to the access provider. We will see in the next section the mutual authentication of two nodes, which reuses the previous authentication scenario (single node to provider) for both nodes.

Within this paper a device that does not explicitly support the cellular network is referred to as "Non-Cellular Node" (NCN), and the device that supports the cellular network as "Cellular Node" (CN). An interconnection of devices belonging to the same person is often treated as a Wireless Personal Area Network (WPAN). The IEEE is putting standardization efforts for WPANs in their 802.15.x workgroup [9]. There is a special focus on the specification and standardization of new physical and link layers to provide short range radio with different bandwidth utilizations and power consumption. The most known outcome of these efforts up to date is the definition of the Bluetooth stack. This stack includes mechanisms for wireless service detection for Bluetooth enabled nodes within the neighborhood. For the following analysis of the different use cases, we assume, that the devices belonging to the same WPAN are preconfigured to form one private network and therefore we suppose the NCN to be able to securely access the cellular services offered by a CN within the same WPAN.

Required Actions to Successfully Establish a Secured Connection Between Mobile Nodes

We focus on the information exchange needed to establish a VPN connection between the nodes, even though commonly VPNs are set up between clients and the concentrator (VPN server), a VPN can also be set up between two nodes to secure their exchanges. The use cases gradually increase in complexity while allowing more general applicability and less user interaction. The ongoing trends towards trusted operators [10] are encouraging the reuse of the cellular network infrastructure to provide authentication and billing services. In the context of heterogeneous networking we focus on the authentication and location of mobile nodes and the secured delivery of the needed signaling information over the cellular network to enable the establishment of secured broadband channels. Figure 2 depicts the separation of the signaling and data channel in the case of short range and peer-to-peer broadband wireless technology like WLAN or Bluetooth. In such a deployment, the mobile nodes are always connected to the cellular network and therefore always reachable for signaling messages.

There are different possibilities to use the cellular infrastructure to provide the authentication service and to transfer signaling information between the mobile nodes. One simple and secure way to do this would be the use of the cellular Short Messaging Service (SMS, a service that allows mobile subscribers to both send and receive alphanumeric messages up to 160 characters long.) to distribute information among the mobile nodes involved in the ad-hoc network. In this case, the

operator's contribution would be limited to the secured distribution of the signaling information between the participants (the CNs are authenticated by the operator based on the SIM and the owner of the CN by the PIN when connecting to the cellular network). The main advantage of this scenario has its biggest effect when the mobile nodes do not have any prior security relation between each other. Then the trust chain is established via the cellular operator having a security association with each of his customers [11]. Other options, like IP over GPRS or USSD services to replace SMS exchanges are currently being worked out.

For example one Mobile Node (MN1) trusts the operator and sends security information, like a session key for a broadband link, via SMS to a second Mobile Node (MN2). The only information MN1 needs is the mobile subscriber phone number (MSISDN) of MN2 to successfully send the SMS, depicted in Figure 1. The SMS can be secured with the security mechanisms provided by the cellular network like the session key (Kc) derived from the shared key (Ki) stored on the SIM card and on the authentication server (AuC).

In the scenario where the data channels used between the nodes are not direct peer-to-peer links, the interconnection takes place via broadband access providers, as in Figure 2, via Bluetooth and WLAN access points. This might be the normal case when the nodes are not situated close to each other. For the establishment of a secured broadband communication channel between the mobile nodes this situation is pretty similar to the former scenario. The main difference consists in the information needed by the peers. As the connection is established with the help of access providers, this information must contain at least a reachable communication address. Most likely the network will be based on IP and thus this communication address will be a global IP address assigned by the access provider. Additionally to this mandatory information, optional information describing the characteristics of the data channel can be added, like the bandwidth or QoS parameters.

In the case, where one mobile node is not connected to a broadband access network, it is possible that the initiating mobile node sends a request to its peer to setup broadband access and report the obtained IP address.

The main drawback of the architecture described in the previous paragraphs is probably the limitation that a node must be connected to a cellular network, called Cellular Nodes (CN). The cellular awareness is required for the exchange of signaling information to setup the secured communication between mobile nodes. In other words, there has to be a mean to securely reach a given node without having more information than a cellular identifier of that node (i.e., the MSISDN). In the prior deployments where only cellular nodes were involved, every node had direct access to the authentication and message delivery

A MAIN REQUIREMENT TO MAKE HETEROGENEOUS NETWORKING CONVENIENT IS THE AUTOMATIC CHOICE OF THE MOST SUITABLE COMMUNICATION TECHNOLOGY.

service of the cellular operator by definition. In the mixed environment where also Non-Cellular Nodes (NCNs) are available, they need some support to access these cellular services. To do so the CN has to relay the signaling information between the cellular network and the NCNs. This requires a secured channel between the CNs and the NCNs. For simplicity reasons, we assume that there is a prior security relationship between the NCNs and their CN. This is acceptable, especially in the case of wireless personal area networks (WPAN), where the CN and the

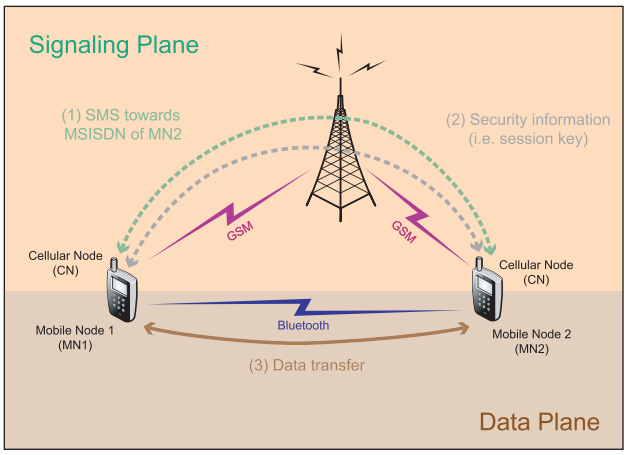

FIGURE 1 Peer to peer signaling between cellular nodes using SMS service.

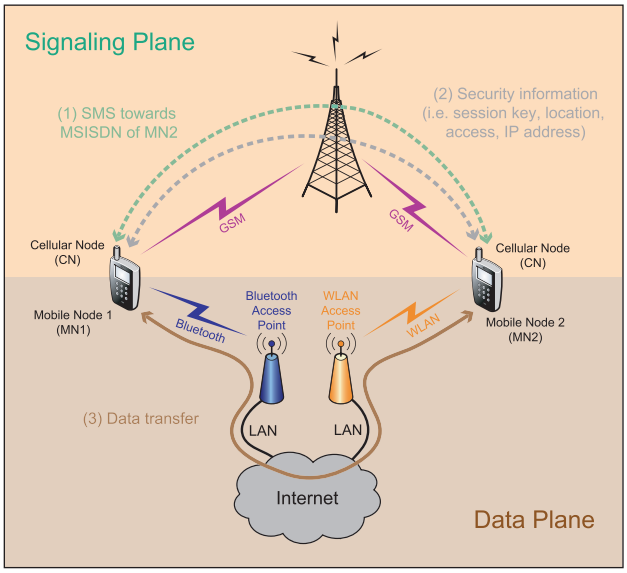

FIGURE 2 Extension to non direct peer-to-peer links with signaling between cellular nodes using SMS service.

THERE ARE DIFFERENT POSSIBILITIES TO USE THE CELLULAR INFRASTRUCTURE TO PROVIDE THE AUTHENTICATION SERVICE.

NCNs form a short range wireless private network and the security association between the devices is pre-established by one administrative authority, i.e., the user that administrates these nodes.

To clarify the steps involved in an establishment of a secured connection among NCNs, an example is presented. This use case involves two users having at least one NCN and one CN each. Namely the first user owns NCN1 and CN1 and the second NCN2 and CN2. The CNs could be standard mobile phones that support Bluetooth for local communication within the WPAN. The NCNs are assumed to support Bluetooth as well to communicate with the CN, and at least one broadband wireless communication technology as data channel. In the presented example the first person would like to establish a secured communication link from her or his NCN1 to the second user. To start the setup, the first user triggers his NCN1 to acquire broadband wireless access. She or he does not have any further information than the MSISDN of the second person (MSISDN2); she or he sends a connection request from his NCN1 via CN1 to CN2. This request includes the IP configuration of the wireless broadband access of NCN1, and her or his MSISDN. The transfer of this request is made in two steps. The whole message exchange is depicted in Figure 3.

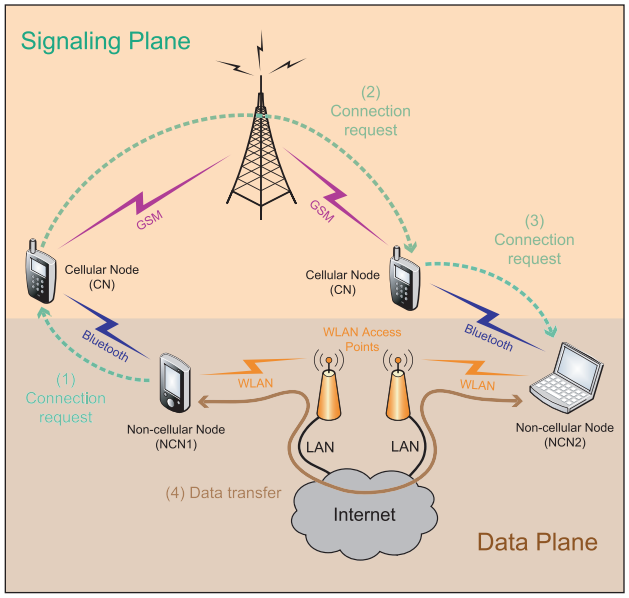

FIGURE 3 Example of generic request to send a file between two non cellular aware nodes.

First, NCN1 sends the request through an a priori secured Bluetooth channel, which is part of the WPAN setup, to CN1. Then it is relayed via the cellular network to CN2. As mentioned earlier, this relaying might happen by using the short messaging service (SMS) of the cellular network. Upon receiving the connection request on CN2, the second person can decide if she or he wants to accept or reject the request. In the case of acceptance she or he can choose the device that should be used for the communication (in the case of having multiple NCNs in his WPAN). The mobile phone of the second person then forwards the connection request to the selected device (NCN2), which in turn tries to connect to a broadband wireless network and returns the resulting configuration to CN2 (connection reply). In the case of an IP based access network, for example, the device reports back the resulting IP configuration. This information is then included into the connection reply and sent back to the originator of the connection request (NCN1). Finally, NCN1 has enough information collected to calculate the security credentials to establish a secured connection towards NCN2. These credentials can again be delivered via the cellular network.

As mentioned before, the signaling can contain optional data. Assume that in this example user 1 intends to send a file to user 2. As optional data, the tape and the size of the file to be transferred could be included. This would help user 2 to choose his device (i.e., his PDA in case of a small file) according to the additional parameters.

Heterogeneous Technologies Networking Assisted by Cellular Networks

The previous use cases become even more interesting, when the participating nodes have different communication interfaces. For example, several people meet in a (conference) room and want to share some data among different mobile nodes. This situation seems to be fairly similar to the previous scenario except for the use of different broadband communication technologies to interconnect all the participating nodes. This heterogeneous interconnection might be based on links of different technologies like infrared (IR), Bluetooth, WLAN, and even wired ones like Ethernet. Because of the increasing variety and complexity of these communication technologies, it becomes more and more difficult for ordinary users to interconnect different devices. Our proposed solution [12] can help to overcome this problem. If the signaling channel offered by the cellular network is also used for the information collection about the available network interfaces of the participating devices it is possible to elaborate a network topology to interconnect all the different mobile nodes within a heterogeneous network. Note that devices having

more than one network interface could be configured as gateways to interconnect devices that do not support the same communication technologies or that are not within the range of each other. For all these different scenarios the degree of integration of the operator can vary. The operator's role can be adjusted from just an enabler, by the use of the SMS subsystem, up to a full integration, where the operator calculates the needed configuration and security information for such a secured heterogeneous interconnection and distributes it to the appropriate participants.

Protocol Design and Implementation Architecture

After having described the different benefits of a Cellular Assisted Heterogeneous Networking (CAHN) framework, this section focuses on the architectural design of CAHN. Considering the fact, that the main idea of CAHN is the authenticated exchange of security and configuration parameters among (mobile) nodes having heterogeneous networking capabilities, it is not surprising that the main part of the CAHN architecture is a communication protocol suite. This protocol consists mainly of three different message types, a connection request, a connection reply and an error reply. These messages are divided in three parts, the header, the cellular header and the service specific data. The header contains basic protocol information like the PDU_ID and the message length, the cellular header contains the parameters needed for the cellular network and the service specific data contains the information related to the used data technology. Figure 4 shows the message format of a Bluetooth connection request and a Bluetooth connection response. The service specific data can be optional in the error response, depending whether the error is service specific or not. Because of the flexible design of the message PDUs the size of them can vary. In a reference implementation [13], where a Bluetooth link was used as data channel, the connection request was 50 characters long and the connection reply contained 60 characters.

The following paragraph is intended to explain the architecture realized to implement and enable the formerly defined protocol. The entity handling this CAHN protocol is called **CAHN Communication Module (CCM)**. The CCM of the CN is extended with functionalities to manage the different NCN devices belonging to the WPAN. These extensions include a database storing

THE HETEROGENEOUS INTERCONNECTION MIGHT BE BASED ON LINKS OF DIFFERENT TECHNOLOGIES LIKE INFRARED (IR), BLUETOOTH, WLAN, AND EVEN WIRED ONES LIKE ETHERNET.

detailed information about the capabilities (i.e., CPU performance, networking devices, display characteristics, Operating System) and the actual status of these NCN devices, that is, if they are reachable at the very moment. The CCM implemented within NCNs is a little bit more lightweight, since the NCNs have only to be able to communicate the CAHN protocol and be aware of their own capabilities.

The CAHN protocol was designed to carry security and configuration parameters over different channels. The first two target channels are SMS and Unstructured Supplementary Services Data (USSD). Because of the different characteristics of these communication

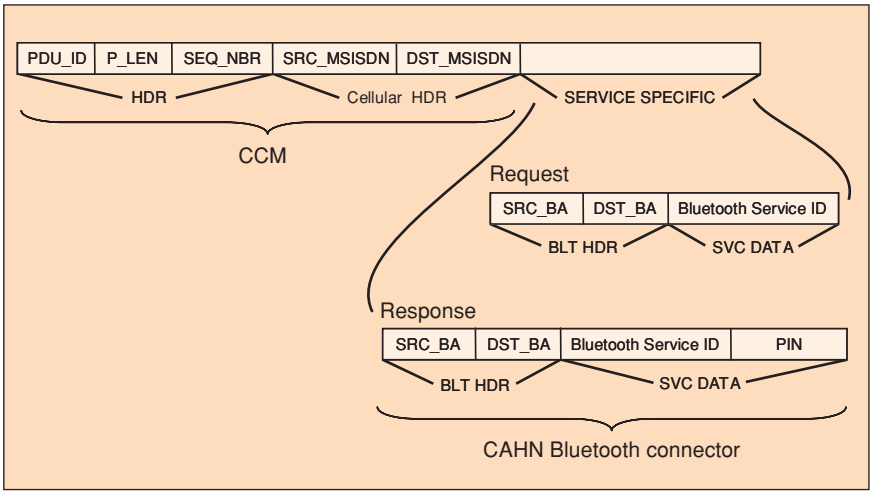

FIGURE 4 CAHN protocol PDUs for Bluetooth.

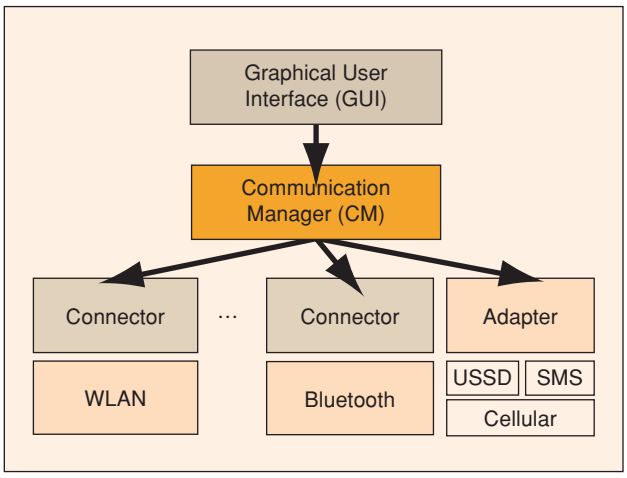

FIGURE 5 The CAHN implementation architecture.

channels we decided to implement so called adapters to appropriately format the CAHN Packet Data Units (PDUs). Using SMS for example, the adapter splits the PDU into messages according to the allowed number of characters. In a standard CAHN communication, CAHN PDUs are not only transmitted via the cellular network between CNs, but also between the CN and NCNs within the WPAN, where often IP is used to communicate. Therefore, the adapter has to cope with different addressing schemes, namely MSISDN and IP addresses. To correctly use the exchanged security and configuration parameters, one other component is required in the CAHN architecture. This component is referred to as connector and is responsible to configure the networking stack according to the formerly negotiated values to get the data plane connected. Due to the variety of parameters that have to be processed for different communications network adapters, there is a CAHN connector for each technology. This separation facilitates the integration of new communication technologies. The different CAHN connectors just have to be registered to the CCM. Whenever security and configuration parameters are negotiated for a particular connection type, the CCM extracts the connector specific part out of the CAHN PDUs and relays it to the right connector. Finally, there is the Graphical User Interface (GUI) component connected to the CCM. Every CCM (on CN as well as on NCN) offers an interface to the GUI to enable any kind of user interaction. Since the architecture on CN and NCN is similar, any CAHN scenario can be initiated either using the CN or a NCN.

The minimal set of components a CN needs consists of a CCM, a WPAN communication adapter (for example Bluetooth) and the appropriate CAHN adapter. In that case the complete user interaction is done on the NCN and the CN is only used as a gateway to the cellular system. Figure 5 shows the implementation architecture.

A case study using Bluetooth technology has been reported in [13], where SMS was used to enable the communication between two non cellular nodes (two computers) via their corresponding cellular phones.

Conclusion

In this paper we proposed to reuse the cellular network for the signaling plane to enable the networking infrastructure of a heterogeneous networking environment. We first studied the secured mobile communications topic, with the signaling channel for authentication and for the exchange the security parameters. We have presented our vision of a convenient wireless networking where a group of devices with different communication technologies (like WLAN, Bluetooth, Infrared, GPRS, etc) can communicate with each other, without the explicit configuration by the end user. This vision leads to the positioning of the cellular operator as the key player in the signaling for the ad-hoc networking configurations. This proposal is quite aggressive for a pure ad-hoc networking vision, where by definition there should be no managed infrastructure. Our genuine approach is based on the user's trust in the cellular operator, and it only inserts the cellular operator for the signaling part, leaving the data transaction as the same procedure as in ad-hoc networking. We have analyzed in detail and with examples different scenarios where a secure connection for communications is established. We have developed the first system architecture for a cellular assisted heterogeneous networking platform that will allow us to build a first implementation of the signaling messaging, and to deploy the first services onto this platform. In a next step the platform will be extended to cope with multihop scenarios, where the intermediate nodes are also configured via a cellular system. Especially in the domain of real time end to end applications like voice over wireless LAN, we are convinced that Cellular Assisted Heterogeneous Networking can help to establish and maintain the heterogeneous multi-hop connections. A first implementation has already been reported using Bluetooth technology and a future WLAN setup is currently being work out.

References

1. Wireless LAN medium access control (MAC) and physical layer (PHY) specification. Institute of Electrical and Electronics Engineers (IEEE), Standard 802.11, 1997.
2. Bluetooth SIG. Specification of the Bluetooth System. (Version 1.0 B), 1999.
3. J. Cai and D.J. Goodman, "General packet radio service in GSM," *IEEE Communications Magazine*, Oct. 1997.
4. S. Mäkinen, R. Kehr, R. Schmitz, F. Vieira, T. Wall, and P. Windirsch, Deployment of Jini Services in an insecure environment. Nov. 2001, Eurescom Project Results.
5. S. Buchegger, J.-Y. Le Boudec, L. Buttyan, and J.-P. Hubaux (eds.), "Cooperation of nodes: The CONFIDANT approach. Report on a working session on security in wireless Ad-hoc networks," *ACM Mobile Computing and Communications Review (MC2R)*, vol. 6, no. 4, 2002.
6. Mobile Ad-hoc Networks (manet), working group: http://www.ietf.org/html.charters/manet-charter.html
7. G. Wu and M. Mizuno, Communications Research Laboratory, Japan Paul J. M. Havinga, University of Twente, the Netherlands, MIRAI Architecture for Heterogeneous Network IEEE Communications Magazine, pp. 126–134, Feb. 2002.
8. Software Defined Radio Forum, http://www.sdrforum.org
9. IEEE 802.15 Working Group for Wireless Personal Area Networks: http://www.ieee802.org/15/about.html
10. S. Lannerström, Trusted Operator, SmartTrust, Revision: B, Sep. 2002.
11. D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet security association and key management protocol (ISAKMP)," *RFC 2408*, Nov. 1998.
12. M. Danzeisen, T. Braun, D. Rodellar, and S. Winiker, "Heterogeneous network establishment assisted by cellular operators," *Proceedings of the Fifth IFIP TC6 International Conference on Mobile and Wireless Communications Networks (MWCN'03)*, Singapore, Oct. 27–29, 2003.
13. M. Danzeisen, D. Rodellar, S. Winiker, and T. Braun, Heterogeneous Networking facilitated by cellular networks COMTEC 03/04, March/April 2004, ISSN 1420-3715, pp. 18–21, June 2004. **VT**