Heterogeneous network establishment assisted by cellular operators

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

Abstract: In this paper, we describe a novel architecture to enable a secure communication among mobile devices using different wireless technologies like wireless LAN, Bluetooth, cellular systems or even infrared. Making use of the combination of these technologies for the data transmission and for the signaling of the communication, we analyze several scenarios with increasing complexity. The complete picture appears in the last scenario where all technologies are involved and the network is composed of heterogeneous mobile nodes. The paper also presents a solution for the setup of a secured communication channel (i.e. a Virtual Private Network connection) between several heterogeneous mobile nodes controlled by the cellular network operator. The mobile nodes can be either cellular aware or non-cellular aware in this framework. We propose to setup the heterogeneous network communications via the cellular network using the cellular aware nodes.

Key Words: WPAN, Ad-hoc networks, Cellular, Wireless LAN, Bluetooth

1. INTRODUCTION

Today, mobile wireless networking combines data connectivity with user mobility. Using technologies like wireless LAN [1], Bluetooth [2], or GPRS [3] the users access their data and are mobile simultaneously. In this paper we are concentrating on networking applications that these technologies can enable. 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 of those communication technologies to establish a secured common networking area to share their data. The paper is organized as follows: First we discuss the current situation and the problems users have to face when they want to establish such secured communication channels among their mobile devices. In section 3 we present our vision of future heterogeneous networking. Then the central issue of this paper is exposed in section 4: we propose to use the cellular network to enable the ad-hoc networking setup. The discussion on different case studies in section 5 makes this proposal more concrete and allows better understanding and positioning of the whole framework for this study. In section 6, we conclude and give some remarks on future work.

2. SECURED MOBILE COMMUNICATIONS

When users want to establish a secured connection among 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 SSID and the used channel 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. The mostly used mechanisms for that are based on shared secrets; the involved mobile nodes have to know a certain value to proof their authorization to establish the secured communication.

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 authentication mechanism and 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 should also happen in a secure way. In most of today's situations, this happens either verbally or by writing down the credentials (Figure 1).

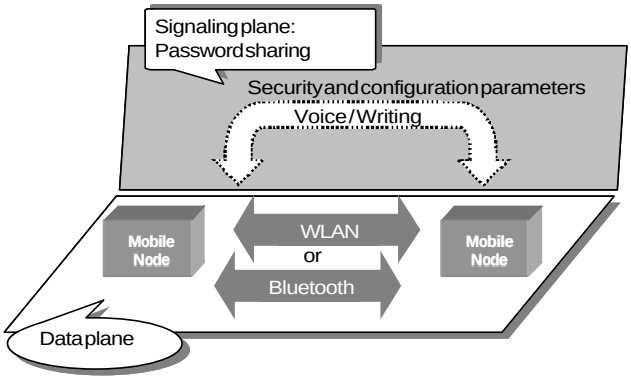

Figure 1 Manual setup of a secured communication between mobile nodes

In this paper we assume that these negotiations of parameters for communication and security form the main part of the signaling needed to build up 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 authentication process and the exchange of securityparameters.

3. A VISION OF CONVENIENT HETERO-GENEOUS 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 successfully transfer a file from one of their devices to a device of a certain person. Furthermore, we think that most users even do not care to which device that file is transferred to, as long as the right person finally has access to that file. This brings up two main requirements for our vision on heterogeneous wireless networking. First, mobile devices belonging to one person should also be addressable by an individual identifier of that person, for instance his mobile subscriber phone number (MSISDN). Often the sender 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 application. This abstraction of the destination node to one existing personal identifier helps to overcome the problem of temporary identifier of the different destination nodes. Most of the broadband wireless connection are set up on demand and have therefore only temporary valid identifiers like a leased IP address for instance. So if the sender can reach the receiver by a static, personal identifier, the receiver can trigger the appropriate device to get temporary 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.

4. CELLULAR OPERATOR ENABLES AD-HOC NETWORKING

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 following the suggestion given in [4]

Trust by Definition

This is the easiest way of trust establishment. Legal authorities, big companies (like banks) and operators are often trusted a priori, or by definition.

Trust based on Heuristics

This 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.

Trust by Delegation

In this model, trust is established by the help of entities, with which a trust relationship already exists, and which are guaranteeing the trustworthiness of a third entity.

Trust delegations are made through third parties, with which a trust relationship exists. This relation again is based on one of the three trust models, mentioned above. 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 [5] [9] where no fixed infrastructure is available, the only possibility to anchor a trust relation chain is the application of the 'Trust by Heuristics' model. As mentioned, this model can be hard to deploy. Only with the help of fixed infrastructure it is possible to apply the 'Trust by Definition' model, which is in our view a must for a platform offering commercial services. Consequently, there are several advantages in reusing the cellular infrastructure to manage heterogeneous wireless networking.

In the mobile as well as in the fixed communications there is a strong need of signaling channels to establish and control data communication. In the same way as it is done in the fixed networks we propose to separate the control plane from the actual data plane. We propose to use the cellular network to support 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 play a role of signaling and configuration provider for heterogeneous ad-hoc networks. The mobile operator will locate the related peers, provide the security mechanisms including the authentication. Furthermore the operator's billing system can be reused to charge the establishment of the networking capabilities.

To establish a secured link or a Virtual Private Network (VPN) among 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. This is a very hard constraint since most of today's portable devices, like notebooks or PDAs, do not directly access the cellular networks. A device that does not explicitly support the cellular network is defined as "**non-cellular aware mobile node**" (NCAN), and the device that supports the cellular network is defined as "**cellular aware mobile node**" (CAN).

An interconnection of devices belonging to the same person is often treated as a Wireless Personal Area Network (WPAN). The IEEE is putting standardization effort for WPANs in their 802.15.x workgroup [7]. 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 wireless communication stack includes mechanisms for device and service detection in the neighborhood of Bluetooth enabled nodes.

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 NCAN to be able to access the cellular services offered by a CAN within the same WPAN.

5. ANALYSIS OF THE KEY SCENARIOS

In the following section we discuss the required actions to successfully establish a secured connection between mobile nodes. Therefore we focus on the information exchange needed to establish a VPN connection between the nodes. The use cases gradually increase in complexity while allowing more general applicability and less user interaction.

To overcome the limitations of a restricted reachability, we propose to use a signaling plane with high availability. In our view, a cellular network like GSM meets very well the requirements of such a signaling medium because of its high availability, because of the built-in security mechanisms and because of the provided always-on feature.

The ongoing trends towards trusted operators [8] 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.

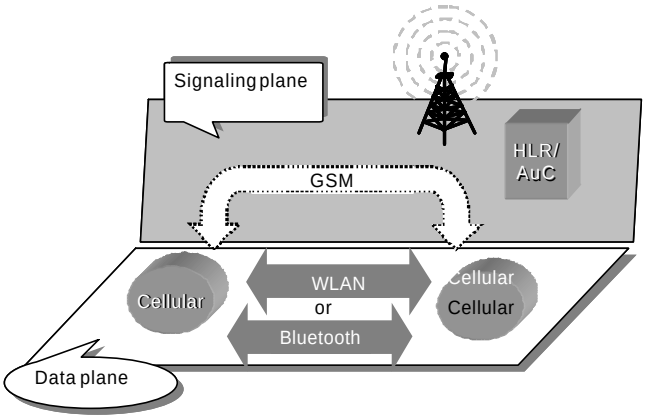

Figure 2 Signaling via cellular operator and data channel via wireless LAN or Bluetooth

There are different possibilities to use the cellular infrastructure to provide the authentication service and to transfer signaling information between the mobile nodes. Probably, the simplest way to do this would be the use of the standard cellular messaging subsystem service (SMS) 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 CANs are authenticated by the operator based on the user's PIN when accessing 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 built up via the cellular operator having a security association with each of his customers [6].

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 the MN2 to successfully send the SMS. The SMS can be secured with the security mechanisms provided by the cellular network like the shared Key stored on the SIM card and on the authentication server (AuC).

In the scenario where the data channels used between the nodes are not peer-to-peer links, the interconnection takes place via broadband access providers. This might be the normal case when the nodes are not situated in the same location. For the setup of a secured broadband communication channel between the mobile nodes this situation is pretty similar to the former scenario. The main difference is the additionally needed information about the location and/or access used by the peers. This can include the IP addresses obtained by the broadband access provider, but also the characteristics of this data channel.

In the case, where one mobile node is not connected to a broadband access network, it is even imaginable 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 sections is probably the limitation to cellular supporting nodes (CAN). The cellular awareness is required for the exchange on signaling information that is needed 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 CANs were involved, every node had direct access to the authentication and message delivery service of the cellular operator by definition. In the mixed environment where also NCANs are available, they need some support to access these cellular services. To do so the CAN has to relay the signaling information between the cellular network and the NCANs. This requires a secured channel between the CANs and the NCANs. For simplicity reasons, we assume that there is a prior security relationship between the NCANs and their CAN. This is acceptable, especially in the case of wireless personal area networks (WPAN), where the CAN and the NCANs form a short range wireless private network and the security association between the devices is established by one administrative authority. In the following figure, this hierarchical approach to extend the signaling to NCANs is shown.

To clarify the steps involved in a setup of a secured VPN among NCANs, an example is presented based on the scenario depicted in Figure 3 with a closer look at the required infrastructure and the exchanged messages.

This use case involves two people having at least one NCAN and one CAN each. Namely the first person owns NCAN1 and CAN1 and the second NCAN2 and CAN2. The CANs could be standard mobile phones that support Bluetooth for local communication. The NCANs are

supposed to support Bluetooth as well, and at least one broadband wireless communication technology.

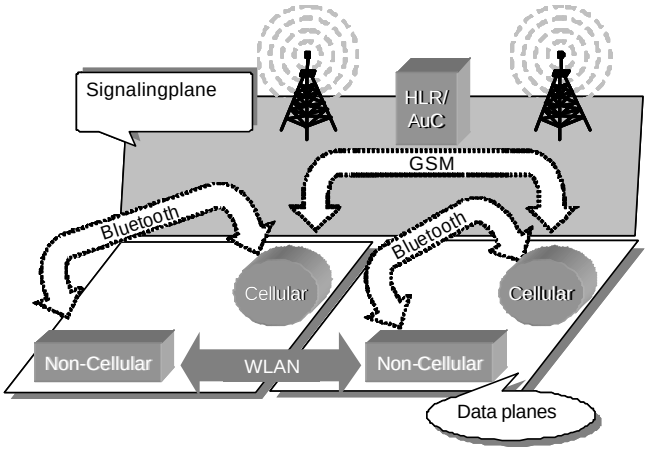

Figure 3 Data transfer between non-cellular aware nodes in the differentlocations scenario

The first person would like to send a file from his NCAN1 to the second person in a secured manner. Therefore he triggers his NCAN1 to acquire broadband wireless access. He does not have any further information than the MSISDN of the second person (MSISDN2); he sends a file send request (*fs_req*) from his NCAN1 via CAN1 to CAN2. This *fs_req* includes the IP configuration of the wireless broadband access of NCAN1, his MSISDN, the type and size of the file to transfer. The transfer of this request is made in two steps. The whole message exchange is depicted in Figure 4.

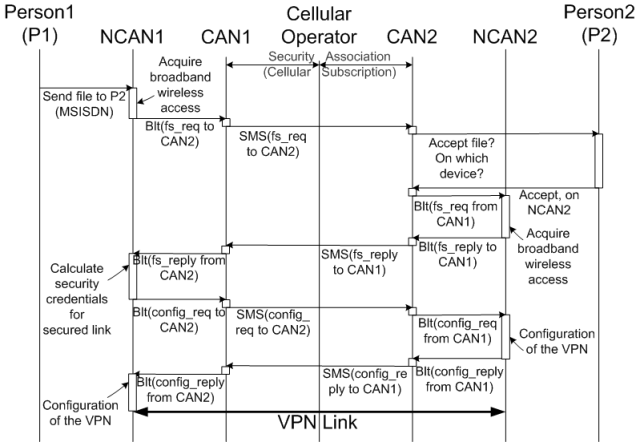

Figure 4 Message exchange between NCAN1 and NCAN2 using CAN1 and CAN2 for the VPN

First, NCAN1 sends the request through a prior secured Bluetooth channel, which is part of the WPAN setup, to CAN1. Then it is relayed via the cellular network to CAN2. As mentioned earlier, this relaying might happen by using the short messaging service subsystem (SMS) of the cellular network. Upon receiving the *fs_req* on CAN2, the second person can decide if he wants to accept or reject. In the case of acceptance he can also choose the device that should receive the file (in the case of having multiple NCANs in his WPAN). The mobile phone of the second person then forwards the *fs_req* to the selected device (NCAN2), which in turn tries to connect to a broadband wireless network and returns the resulting configuration to CAN2 (*fs_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 *fs_reply* back to the originator of the file send request (NCAN1). Finally, NCAN1 has enough information collected to calculate security credentials to establish a VPN connection towards NCAN2. These credentials can again be delivered via the cellularnetwork.

HETEROGENEOUS TECHNOLOGIES NETWORKING ASSISTED BY CELLULAR NETWORKS

The previous use case becomes even more interesting, when the participating nodes have different communication interfaces. For example, several business people meet in a conference room and want to share some data among different mobile nodes. This circumstance seems to be fairly similar to the previous scenario except for the use of direct broadband connections between the participating nodes. These direct connections are built on a combination of different technologies like infrared (IR), Bluetooth, WLAN, and even wired links 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 can help to overcome this problem. If the signaling channel offered by the cellular network is also used to collect information about the available network interfaces of the participating devices it is possible to calculate a network design to interconnect all the different mobile nodes within an heterogeneous network. Figure 5 shows such a heterogeneous network using the different network interfaces available on the NCANs.

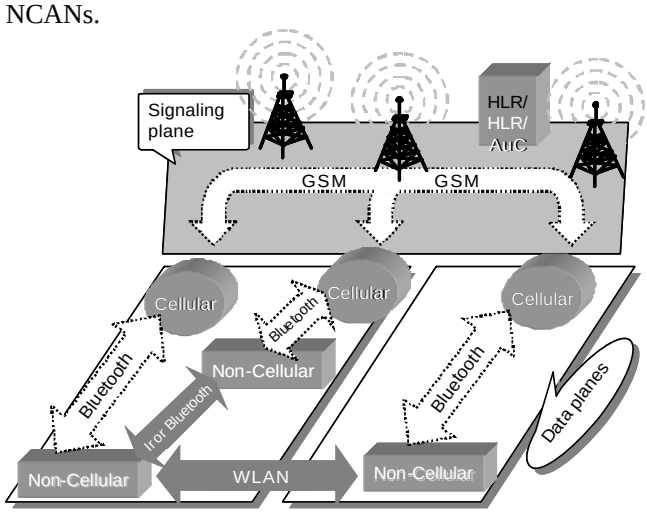

Figure 5 Heterogeneous technologies networking assisted bycellularnetworks

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 and distributes it to the appropriate participants.

6. CONCLUSION

In this paper we propose to reuse the cellular network for the signaling plane to enable the networking infrastructure of an heterogeneous networking environment. We first studied the secured mobile communications topic, with the signaling channel for authentication and for exchanging 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 together, without the explicit configuration by the end user. This vision leads to the statement of the cellular operator as the key player in the signaling for the ad-hoc networking configurations. This proposal is quite aggressive for a follower of pure ad-hoc networking, 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 an 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.

REFERENCES

[1] WLAN IEEE 802.11, http://grouper.ieee.org/groups/802/11/main.html

[2] Bluetooth SIG, http://www.bluetooth.org/

[3] General Packet Radio Service in GSM. Jian Cai and David J.Goodman. IEEE Communications Magazine, Oct.1997.

[4] Deployment of Jini Services in an insecure environment, Susanna Mäkinen, Roger Kehr, Roland Schmitz, Frederico Vieira, Tom Wall, Peter Windirsch, http://www.eurescom.de/public/projectresults/P1000-series/1005D6ti5.asp

[5] "Cooperation of Nodes: The CONFIDANT Approach - Abstract." Sonja Buchegger and Jean-Yves Le Boudec, Levente Buttyan and Jean-Pierre Hubaux (eds.), 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] Internet Security Association and Key Management Protocol (ISAKMP), http://www.ietf.org/rfc/rfc2408.txt

[7] IEEE WPAN Workgroup, http://grouper.ieee.org/groups/802/15/

[8] "Trusted Operator" Sten Lannerström, SmartTrust, Revision: B, September 19, 2002, http://www.smarttrust.com/trustedoperator/trustedoperator.pdf

[9] Mobile Ad-hoc networks (manet), http://www.ietf.org/html.charters/manet-charter.html