Heterogeneous Networking facilitated by cellular Networks

MARC DANZEISEN, DANIEL RODELLAR, SIMON WINIKER AND TORSTEN BRAUN **A mobile ad-hoc network is a collection of wireless terminals that can be deployed rapidly and is self-organising. Integrating ad-hoc networks with a well-established cellular network can improve communication and security, as well as enrich the cellular services. How can secure data communications based on temporarily acquired broadband access between two users not knowing each other be achieved?**

In this article we show that it is possible to perform such a secured communication using a user-friendly setup via a cellular network. We promote a secure connection between two users on any wireless network technology (i.e. Wireless LAN, Bluetooth) with easy installation and setup reusing the cellular network. The novelty of our concept is an original architecture and an innovative model based mainly on the usage of the Wireless WAN network to locate, authenticate users and exchange keys to secure the heterogeneous links between the mobile nodes. In our architecture the mobile nodes can be either connected directly to a cellular network or indirectly via other nodes. A description of the implementation using the Bluetooth technology in a given scenario will be presented.

Introduction

Today, mobile wireless networking combines data connectivity with user mobility. Mobile users access their data using technologies like wireless LAN [1], Bluetooth [2], or GPRS [3]. In this article 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 of those 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 an example: John has two personal communication devices: 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 John 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 they are physically far from each other, or there is no trust relationship between them, we propose a service framework to exchange the security and configuration parameters to establish a secure connection and to securely transfer the document in an easy and user-friendly way. Therefore, John sends a service request to Alice's mobile phone, she then decides to which broadband device the file has to be transferred (laptop or PDA, for example). The proposed system triggers this chosen device to acquire network connectivity (LAN, WLAN, Bluetooth, or any other network access to the Internet). Finally, John and Alice are able to let their devices exchange the document.

Secured Mobile Communications

When users want to establish secure connections between their mobile devices, 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 such as the operation mode (Infrastructure or Ad-hoc) and the SSID have to be set before the devices become visible to each other.

Assume that John wants to transfer a file from his laptop to Alice, who is in the same room using Bluetooth. Even if John can see that the person sitting next to him is Alice, he can not be sure that the Bluetooth device his laptop is communicating with really does belong to Alice and not to somebody else sitting in the very next room. What is needed to resolve uncertainty is a method to prove that the chosen Bluetooth device actually belongs to Alice. The simplest and thus most widely used mechanisms for that are based on shared secrets; the involved mobile nodes have to know a certain value to prove their authentication before establishing the secured communication. In most of today's situations, this happens either verbally or by writing down and manually configuring the credentials.

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 features further information has to be negotiated such as 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 information exchange should also happen in a secure way.

In this article we assume that these communication and security parameter negotiations form the main part of the signalling needed to establish a secured private connection between mobile nodes. In the case of a self-organising

technology like Bluetooth, where the nodes are able to discover their neighbourhood and automatically establish a communication link, the signalling information is reduced to the authentication process and the exchange of security parameters.

Trust is the basis for every authentication process. Trust is the result of applying one of the three models: trust by definition, by delegation (e.g. A knows B, and B knows C, so A trusts C) or by refinement. Trust can be delegated: trust can build upon an existing trust relation. This can result in so-called trust chains, where trust has been continuously delegated. As with every chain, these trust chains are only as strong as the weakest link. Every trust chain has to have an origin trust relation. This trust relation is the anchor of the chain and can only be achieved by applying one of the two models: trust by definition or by refinement. Authentication mechanisms based on the trust by refinement model are hard to implement. The trust by definition model will be applied for authentication in the framework described here. This has the impact that infrastructure is needed and an entity has to be present in the network as an enabler for the application of the trust by definition model.

A Vision for convenient heterogeneous Wireless Networking

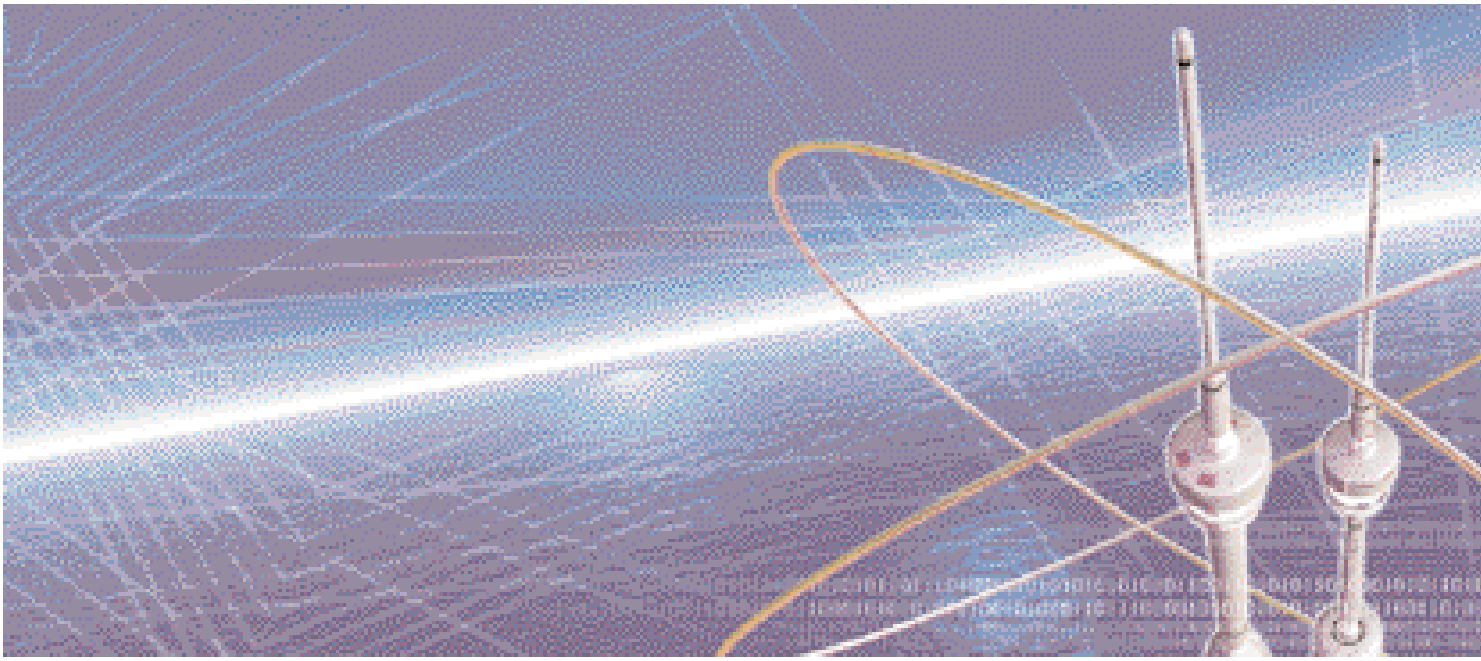
We believe that users do not want to be aware of all these different configuration and security issues. End users just want to securely transfer a file from one of their devices to a certain person. This creates two main requirements for our vision on heterogeneous wireless networking. First, each user needs his own individual identifier, for instance his mobile subscriber phone number (MSISDN). 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 transfer. This abstraction of the destination node to one existing static personal identifier helps to solve the problem of dynamic identifiers of different destination nodes. Most present wireless broadband connections are charged based on time and therefore connected on demand, having only temporary valid identifiers like dynamic IP addresses. This restricted reachability can be improved using a signalling plane with high availability that is always on. 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 perform 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 cost. This is of prime importance when the nodes involved are interconnected by the help of access providers. The selection of the technology will also be of high importance to assure optimised resource management.

Heterogeneous networks are networks in which the nodes do not share a single common access technology. The main problem to establish a connection in heterogeneous networks is the exchange of the required connection parameters, such as in the general scenario depicted in figure 1. The same also applies to establish a secured connection. This initial bootstrapping problem is hard or perhaps impossible to solve in fully distributed scenarios. For that purpose we suggest to separate the signalling plane from the data plane. The signalling plane can then be used to exchange the required connection or security parameters.

The suggested signalling plane uses a cellular network for the transport of signalling messages. The GSM network distinguishes itself by its high reachability. The low bandwidth is not a drawback as the data will still be transferred over broadband links, and for the signalling information not much bandwidth is required. On the other hand, the existing trust relation between the operator and the clients of the cellular network can serve as a basis for authentica-

Heterogeneous networks are networks in which the nodes do not share a single common access technology.



tion. The high reachability again makes this authentication feature almost pervasive, which is a big advantage for spontaneous networks. And, last but not least, the operator's billing system can be reused to enable the users of the envisioned platform offering commercial services.

Cellular assisted heterogeneous Networking Implementation realised in a Bluetooth Environment

Bluetooth basic Concepts

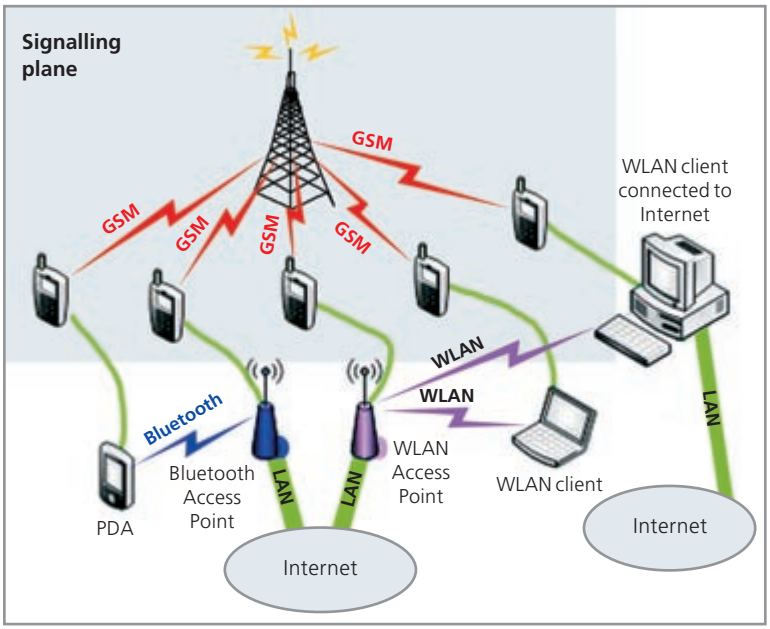
In a Bluetooth environment devices scan the environment for other Bluetooth devices. For that purpose a message is periodically spread on different frequencies. Bluetooth can also help to discover services on other devices. To achieve this Bluetooth defines its own Service Discovery Protocol (SDP). Services can either be detected on a known device to get the list of the capabilities of the detected device, or services may be searched in the environment. In both cases the inquiry can be involved to get available devices. In order to be able to announce services and detect services, a common description must be defined in advance. This is achieved by using profiles. Such profiles describe a service in detail. Profiles are standardised through the Bluetooth Special Interest Group (SIG). Devices enabled with a certain profile can announce this capability and detect other devices with this capability.

Devices can be hidden when they are in an undiscoverable mode. In order to protect the services Bluetooth implements its own security model for the access. With the help of this model nodes can be authenticated and links can be encrypted. The Bluetooth security model defines three modes for security.

– Security Mode 1: No Security procedures are enforced and the access is not restricted.
– Security Mode 2: A device does not initiate security procedures before channel establishment. This mode allows different and flexible access policies for applications, especially to run applications with different security requirements in parallel.
– Security Mode 3: A device initiates security procedures before the link setup is completed. In this mode it is not even possible to exchange SDP messages (link level enforced security).

These security modes are the basis for every connection attempt. In order to set up a link corresponding to the security mode needed, the accessing device must be authenticated. This authentication is based on a PIN (Personal Identification Number). Furthermore, the PIN is used to generate a link key, which then forms the basis for the encryption key, which is regenerated periodically during a connection. For a secure connection establishment a link key shared by the devices is needed. If no such link key exists, it has to be generated and therefore the user has to provide a PIN. If the PINs entered on both devices match the link key this will lead to a successful connection establishment. This handshake procedure either happens upon link layer connection establishment or L2CAP (Logical Link Control and Adaptation Layer Protocol) connection establishment, depending on the used security mode.

Fig. 1. Scenario where a secure connection is established between a PDA using Bluetooth and a laptop and a computer (that is connected to Internet), both connected to an access point using WLAN.



Cellular assisted heterogeneous Networking Implementation

Bluetooth Security can be very limited, when no former trust relation exists between the users and no PIN has been defined. We overcome this difficulty by providing a signalling channel to the users for exchanging the required security parameters such as the PIN.

In practice this enables a spontaneous and secured connection establishment to shared services which are security enabled. With the help of the framework described and its authentication feature, the scalability and applicability of Bluetooth can be improved.

The following description of the implementation demonstrates the use of the cellular network in a Bluetooth environment as shown in figure 2. Node A will be a network access point and Node B a client. Both have Bluetooth interfaces. Furthermore Node A has an Internet connection. In order to be able to share this Internet connection Node A has to enable the Personal Area Network (PAN) profile with the defined role of a Network Access Point (NAP). Additionally, bridging mechanisms have to be configured to offer data relaying. On the client side at Node B, an implementation of the PAN Profile must be present too and the device must be set up with the PAN User role.

Node A has to enable security to protect the NAP service. As Node B must be able to detect the service, Bluetooth security Mode 3 can not be used and therefore Bluetooth security Mode 2 was chosen. This mode enables service level security, perfectly matching the defined requirements of this project, where the communication encryption is left to the service implementation and the authentication is provided by the security framework. On both devices a PIN database was implemented, which can be queried for a PIN upon a connection request.

If the user (Node B) is in need of an Internet connection, he can browse his environment for available Access Points.

For that purpose Node B issues an inquiry and scans the availability of other Bluetooth devices. When other devices are found, Bluetooth SDP is used to discover the available NAP services. If Node B tries to connect to that service, Node A will browse its database for a PIN for that specific Bluetooth address and the same happens on Node B. If no common PIN is found in the respective databases, Node B will not be granted access to Node A.

Our framework will be used to send a connection request from Node B to Node A. As the channel for this request is the GSM network, both devices, Node A and Node B must also have an established GSM connection. The request of Node B must also contain the relation between an identifier and the connection end, in this case the Bluetooth address of Node B. With the help of this information Node A can generate a PIN for Node B, update its database and send a connection response including the generated PIN back to Node B, assuming Node B is within reach of Node A (this can be verified with an inquiry). When Node B receives the response, he in turn can authenticate Node A and update its database with the acquired PIN. A further connection attempt is now likely to succeed, as both nodes are now in possession of a common PIN.

In order for Node B to be able to send a connection request, Node A must somehow announce his cellular assisted capabilities to Node B and also his mobile subscriber identifier (MSISDN). For that purpose a new service has to be implemented and added to the Bluetooth SDP, so that Node B can detect the required parameters of the new framework using the Bluetooth SDP. For Node B to be able to understand this capability announcement and parameters, the new service also has to be integrated on the client side (Node B).

Our framework is intended to help with connection and security establishment and to act on behalf of the end user for easy configuration.

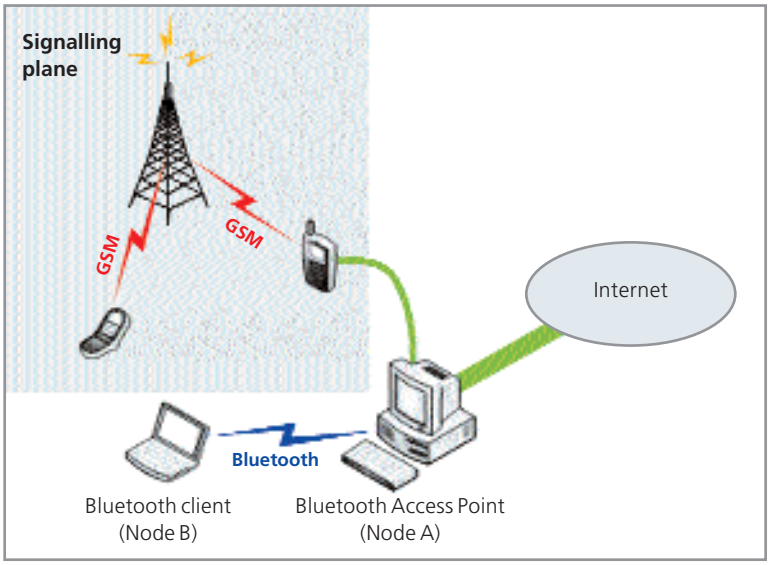


Fig. 2. Scenario where Node B connects securely to Node A using Bluetooth and takes advantage of Node A's connection to Internet.

Conclusion

In today's networks there is a large choice of different access technologies and the trend towards mobile devices. The formation of networks is no longer static and this dynamism introduces significant configuration and management issues. We believe that users do not want to be aware of these different configuration and related security issues. This creates two main requirements for our vision on heterogeneous wireless networking. First, each user needs his individual identifier, for example his mobile subscriber identifier. Additionally, the sender often does not know the device of the receiver. 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 statically existing personal identifier helps to solve the problem of dynamic identifiers of the different destination nodes. The framework in which the cellular network enables the heterogeneous networking is called CAHN: Cellular Assisted Heterogeneous Networking. CAHN is a very promising approach to ease the configuration and management of dynamic networks and can offer a basic authentication, which provides great accessibility. The reuse of broadband links for the data transmission enables the combination of a high bandwidth and low coverage data link with a low bandwidth and high coverage signalling link.

In this article we have described the platform built on Bluetooth access technology (Bluetooth SDP enabled environment) to show the benefits and feasibility of the CAHN framework and its ability to ease the configuration and establishment of spontaneous networks. The platform provides applicable authentication mechanisms as a basis for secure service deployment and service access.

We have developed the first system architecture for a cellular assisted heterogeneous networking platform that will allow us to build implementations of signalling message exchange, and to deploy the first services on to each platform. In a next step the platform will be extended to cope with multi-hop scenarios, where the intermediate nodes are also configured via a cellular system. ■

Marc Danzeisen, Computer Scientist, R&D Consultant, Swisscom Innovations, marc.danzeisen@swisscom.com

Daniel Rodellar, Telecommunication Engineer, Project Leader, Swisscom Innovations, daniel.rodellar@swisscom.com

Simon Winiker, Student in Computer Science, simi@winiker.ch

Torsten Braun, Prof. Dr. at the University of Bern, Computer Networks and Distributed Systems, braun@iam.unibe.ch

Links

[1] IEEE P802.11, Working Group
[2] Bluetooth SIG webpage: www.bluetooth.org/
[3] Jian Cai and David J. Goodman: "General Packet Radio Service in GSM", IEEE Communications Magazine, October 1997.
[4] Marc Danzeisen, Torsten Braun, Daniel Rodellar and Simon Winiker: "Heterogeneous Network Establishment assisted by Cellular Operators", The 5th IFIP TC6 International Conference on Mobile and Wireless Communications Networks (MWCN'03), October 27–29, 2003, Singapore.