IMTC 2004 – Instrumentation and Measurement
Technology Conference
Como, Italy, 18-20 May 2004

A Wireless Network of EIS Devices

Åke Östmark, Conny Öhult, Joakim Eriksson, Per Lindgren, Jerker Delsing
Luleå University of Technology
Department of Computer Science and Electrical Engineering
Division of EISLAB
SE-971 87 Luleå, Sweden
http://www.eislab.sm.luth.se

Abstract *– By using a sensor connected to a generic wireless Embedded Internet System (EIS) platform, data can be presented on-line over the Internet using a standard WWW-browser. When started, the EIS device automatically searches and connects to other devices providing Internet connectivity. The EIS can also provide Internet access for other devices, for example other EIS platforms, thus creating a local network. In this paper we focus on mobile phones with GPRS as the means for wireless Internet connectivity as it provides enhanced area coverage in today's networks. To overcome the problem of non-public IP addresses, a basic server based solution is developed. Our experiments confirm that within GPRS coverage, the EIS device successfully provides Internet access and presents data for on-line monitoring over the Internet.*

I. INTRODUCTION

Today's technology makes wide usage of sensors to get systems working. In this paper, we present a generic wireless Embedded Internet System (EIS) platform, allowing sensors and actuators connected to the EIS to be accessible on-line to the public Internet.

The interoperability of the device is achieved by conforming to common standards, (e.g. Bluetooth, TCP/IP, and HTTP). When started, the EIS device searches and connects to other devices providing Internet connectivity, e.g. cell based or wired access points.

When connected, the EIS device may also provide Internet access for others devices (such as other EIS) in the close proximity of the platform. To support these multiple devices accessing the Internet, we have developed a Network Address Translation (NAT) [1] implementation running on the EIS device(s).

One application area is monitoring patients outside the institutional environment. Sensor data can be monitored in near real-time (and/or logged) while the patient is allowed mobility within the coverage area of the access point. In particular, Internet connection via a Bluetooth/GPRS-enabled mobile phone as access point offers excellent coverage by today's well established cell-based networks.

However, assigning IP addresses to hosts is operator dependent and may prohibit access initiated from the public Internet. To overcome this problem of non-public IP addresses, a basic proxy server based solution is developed.

Our work in progress is demonstrated through interfacing a motion sensor (accelerometer) and a pulse oximetry sensor to EIS platforms. The motion sensor can be used to monitor e.g. activity or body position of a patient while the pulse oximetry sensor provides pulse rate and oxygen saturation (SpO_2) data.

The paper is structured as follows; section II gives an overview of the EIS platform architecture. Section III covers the implementation to support multiple devices connected to the Internet. In section IV, a test scenario is presented and in section V, the paper is concluded.

II. EIS PLATFORM ARCHITECTURE

We extend the EIS-platform concept presented in [2]. The hardware platform in Fig. 1 below is a battery powered embedded systems consisting of:

- a microcontroller, Renesas M16C/62M with 20kB RAM and 256kB FlashROM running at 4.608 MHz [3]
- a Bluetooth module, Mitsumi WML-C10 [4]
- and an interface to connect sensors/actuators

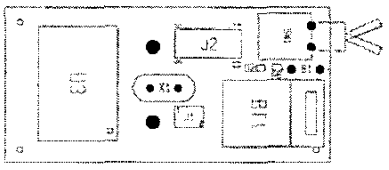

Fig. 1. EIS platform

The software architecture consists of:

- lwIP [5][6], a TCP/IP stack implementation optimized to reduce memory and CPU resources.
- an in-house developed Bluetooth stack, lwBT [7], which extends lwIP with Bluetooth LAN access capabilities such as the LAN Access Point (LAP) and Dial-Up Networking (DUN) profiles [8].
- a web server and sensor application.
- and a real-time operating system, RTXC [9].

0-7803-8248-X/04/$17.00 ©2004 IEEE

A. Enabling Internet access

In [2], we showed that it is possible to access the EIS device from any device supporting TCP/IP and the Bluetooth LAN Access profile. The concept allows user interaction through standardized WWW-browser technology from e.g. a PDA in close proximity of the EIS device. To make it possible to access the platform from practically anywhere, the capability of the platform is improved to use a variety of network access points to obtain Internet connectivity. As access point, the EIS may use e.g. a Bluetooth access point connected to a wired network or a Bluetooth/GPRS-enabled mobile phone.

In this paper we focus on mobile phones with GPRS as the means for wireless Internet connectivity as it provides enhanced area coverage amongst presently available technologies.

One major problem is that the EIS device might not be able to receive inbound connections, initiated from the public Internet. Depending on the network operator, we might be assigned a non-static mapped private IP address and hence, the service offered will never be available from the public Internet.

We use a solution where the EIS device, from the user's point of view, is accessible from virtually anywhere as long as the device is within range of a suitable Bluetooth network access point.

The aim of the architecture is similar to what a user experience when accessing resources on the Internet through a proxy server i.e. all returned responses appears to be directly from the EIS device. When started, the EIS platform accesses a public known server acting as a host for all connected EIS devices. A user requesting a service from a specific EIS platform accesses the public known server. In turn, the server relays the requests to appropriate EIS platform invisibly from the user's perspective. The user requests can be regular HTTP requests to the on-board web server, configuration of the device or accesses to data sampled from a sensor. As a front end to end-users, the server presents a web interface indicating the status of the EIS platform. The web pages are created and modified dynamically when EIS devices connect or disconnects with the proxy server.

In our experimental setup, one proxy server was used during tests. Using only one server has the disadvantage of being the single point of failure, i.e. if it fails, all connected EIS devices will be unreachable. To overcome the single-point of failure, a number of proxies could be set up to achieve redundancy.

One advantage of using a proxy server is to store large amount of data from EIS devices for post-processing and analysis. Moreover, since the proxy server is the single point of entrance, it is very easy to implement security features e.g. access control to the EIS devices.

III. NETWORK ADDRESS TRANSLATION

A Bluetooth enabled mobile phone commonly implements the capabilities of the DUN profile by acting as a wireless modem. One of the restrictions in the DUN profile states that the mobile phone will only allow one Bluetooth connection to gain Internet access using its dial-up or GPRS services.

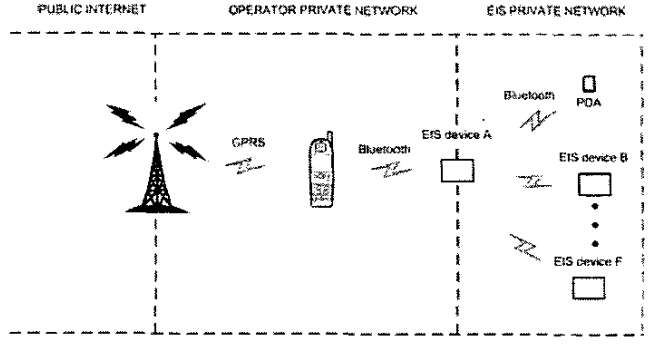

Fig. 2. Network overview

When we, as shown in Fig. 2, connect device A to the GPRS service provider, we get only one valid IP address. Thus device A needs to create a private network and assign its members, device B and the PDA, IP addresses from a private address space. To allow the devices in the private network to communicate with the external network, such as the Internet, we need to multiplex the traffic from the private network and present it to the external network as if it was coming from a single device having only one IP address.

We have implemented a small and generic traditional NAT implementation to be used with lwIP. Our implementation has flexible configuration options which make it suitable for a wide variety of applications while limiting the overhead of unused mechanisms.

The purpose of our implementation is to optimize NAT for lwIP by taking advantage of lwIP's routing capabilities, memory management, and network interfacing. In the following we will refer to traditional NAT as "NAT".

A. NAT overview

NAT processing of packets from local connections use the multiplexing of the TCP/IP stack to ensure that each connection from a node in the private network can be uniquely identified when routed to the external network. NAT has a mechanism that translates the source IP address of the TCP/IP packet coming from the private network destined for the external network, with the IP address which is unique to the external network. To identify incoming packets on the connection it must also translate the Transport identifier (such as TCP/UDP source port or ICMP query ID) to an identifier unique to the connection.

Packets from the external network are parsed by NAT and a session lookup is performed. If the packet contains an assigned unique Transport identifier, the IP address and the identifier is translated before the packet is routed to the private network. All inbound TCP/IP sessions are directed to the NAT router as the end node unless the target Transport identifier is statically bound to a node in the private network.

B. Implementation

The NAT implementation is driven by incoming packets from the network interfaces. If the packet originates from the private network and is destined to the external network a session with a binding is created if needed.

When a packet arrives from the external network, NAT checks the Transport identifier destination to see if the TCP/IP packet should be routed to the local TCP/IP stack or on to one of the private network interfaces.

Because applications will have different views on the best way to end a session [10] we have implemented three (to each other) independent mechanisms. To save code space, any configuration of the following mechanisms can be used.

- The simplest method is to end the longest idle session when the maximum number of allowed sessions has been reached and a new session needs to be created.
- Since TCP sessions are connection based, they can be removed when the connection is closed.
- It may be useful to keep session timeouts for each of the different session types, but this view of session termination should only be used when it coincides with that of the application.

The NAT router node is a member of both the private and external network with a configurable private IP address.

The checksums are adjusted using standard techniques.

We have limited our work to not examine or modify transport payload with application level gateways. For this reason we do not cover applications with IP address content.

IV. TEST SCENARIO

To test an environment using a network of two EIS devices, two sensors for medical applications was connected to each of the devices. Both devices can, as device A in Fig. 2, connect to the Internet through a mobile phone over GPRS. Because the mobile phone only allows one of the devices to be connected, the device that first establishes a connection will act as a NAT router.

When the EIS devices are started, a Bluetooth inquiry is initiated to find devices that provide Internet connectivity. As described in Figure 2, a mobile phone with GPRS and the Bluetooth DUN was used to enable EIS device A to create a RFCOMM connection. The EIS device A then connects the TeliaMobile's, Sweden, GPRS network using standard AT commands and PPP. When the connection is established, the device becomes discoverable and acts as a Bluetooth LAP, thus it allows device B and others, such as a PDA, to gain access to the Internet.

To monitor physical activity and body position, a piezoresistive silicon accelerometer was interfaced to the first EIS device. The sensor is of a piezoresistive silicon type and has a range of ± 50 g. The sensors are delivered with calibration data and the sensor, used in this platform, has 0,871 mV/g in sensitivity at 100 Hz, 5 VDC and 25°C. A measuring range of ± 2,5 g was sufficient for our purposes and to use the full dynamic range of the 10-bit A/D-converter an amplification of 1000 was chosen. This resulted in 0,575 V/g in output with 3,3 VDC supply and the signal-to-noise ratio was measured to be 48 dB.

The sensor measure acceleration in one direction and the low-frequency part of the output signal can be used to determine the body position e.g. vertical or horizontal. The high-frequency part of the output signal can be used to determine the level of activity. Further signal processing can be applied to identify certain movement patterns such as steps. However, during the tests, this was not carried out.

A finger clip sensor with an integrated pulse oximetry module was interfaced by the second EIS device. The sensor provides a constant data rate (three bytes per second) of oxygen saturation and pulse rate values. The pulse rate and oxygen saturation range are from 18 to 300 pulses per minute and from 0 to 100 %, respectively.

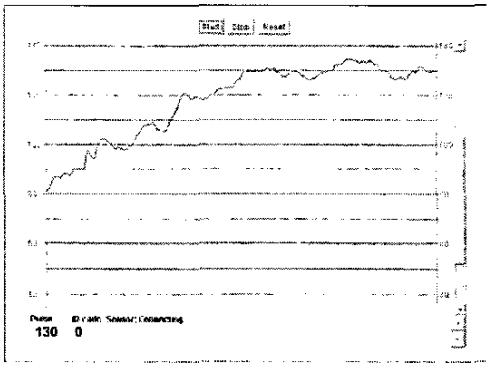

Fig. 3. On-line monitoring the pulse

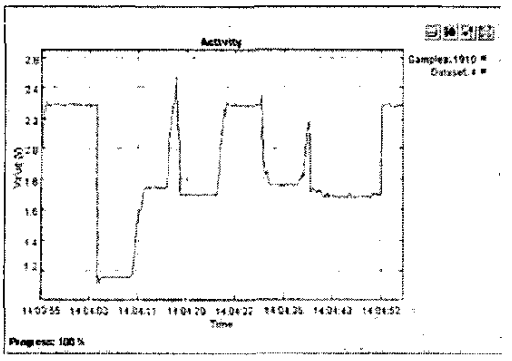

Fig. 4. Sensor data when post-analyzing the activity

During operation, any user interested in sensor data needs to access the on-board web server to download a Java applet. The applet is used for on-line presentation of data to end-users while monitoring a patient, see Fig. 3 above. Sensor data is also forwarded to the proxy server to be stored for post-process analysis, as in Fig. 4 above. Post analysis is also possible while the EIS devices are offline since the presenting software is downloaded from the proxy server. On-line monitoring makes it possible to provide interaction e.g. between a physiotherapist and the patient during therapy. By analyzing the on-line data, the physiotherapist can give instant feedback and advice to the patient. Analyzing data collected from a long period of monitoring makes it possible to detect e.g. irregular patterns of healthy signs.

The current implementation uses TCP as transport layer protocol both for sending sensor data as well as administrative tasks. For on-line monitoring, sending e.g. 3 bytes of oxygen saturation and pulse values, more than 90% of the transmitted data is due to the TCP/IP packet header overhead if every sample is sent in an IP packet on its own. This has a negative impact on the power consumption since radio transmission is a major power consumer [11]. If possible, UDP can be selected as transport protocol in order to reduce radio transmission, but then there is no guarantee that collected samples ever reach their destination.

V. CONCLUSIONS & FUTURE WORK

Our experiments confirm that within GPRS coverage, the EIS platform successfully provides Internet access and presents data for on-line monitoring over the Internet.

The use of TCP/IP connectivity over GPRS allows interaction with the mobile EIS through a standard WWW-browser, thus eliminating the need for deploying proprietary protocols and applications. An EIS device can create a private network if needed, providing access for other devices.

The current lwBT implementation only allows for one device to act as a Bluetooth LAP in a private network. To enable DT (Data Terminal) devices, which are connected to a LAP, to act as LAP's, themselves, the DT need to negotiate low power modes with the LAP. This will enable the DT to act as a LAP in a private network of its own, allowing us to create multiple layers of private networks.

Increasing the operational lifetime of the EIS devices can be achieved by using various header compression schemes to reduce the TCP/IP header overhead and hence, power consumption. Other factors presented in [11][12] should also increase the lifetime of the EIS device, such as various operating modes of the MCU and Bluetooth module.

One key issue in the presented paper is, even though the proxy architecture decouples the clients from the EIS network, both sides are running the standard TCP/IP protocol suite.

VI. REFERENCES

[1] P. Srisuresh and K. Egevang. "Traditional IP network address translator (Traditional NAT)". RFC 3022, Internet Engineering Task Force, January 2001.

[2] Å. Östmark, L. Svensson, P. Lindgren, J. Delsing, "Mobile Medical Applications Made Feasible Through Use of EIS Platforms". *IEEE Instrument and Measurment Technology Conference*, pp. 292-295, May 2003

[3] Renesas, microcontroller M16C/62M
Web page: 2004-03-01
URL: http://www.renesas.com

[4] Mitsumi, Bluetooth module WML-C10
Web page: 2004-03-01
URL: http://www.mitsumi.com

[5] A. Dunkels. lwIP – a lightweight TCP/IP stack.
Web page. 2003-10-11.
URL: http//www.sics.se/~adam/lwIP/

[6] A. Dunkels. Full TCP/IP for 8-bit architectures.
Swedish Institute of Computer Science,
April 2002

[7] C. Öhult. lwBT – a lightweight Bluetooth stack.
Web page. 2003-10-11.
URL: http://www.sm.luth.se/~conny/lwBT/

[8] Bluetooth Special Interest Group. Bluetooth Core, Specification of the Bluetooth System, Version 1.1. February 2001.

[9] Quadros Systems, Inc.
Web page: 2004-03-01
URL: http:// http://www.quadros.com/

[10] P. Srisuresh and M. Holdrege. IP network address translator (NAT) terminology and considerations. RFC 2662, Internet Engineering Task Force, August 1999.

[11] V.Raghunathan, C. Schurgers, S. Park, M. B. Srivastava. "Energy-Aware Wireless Microsensor Networks". *IEEE Signal Processing Magazine*, 19(2) pp. 40-50, 2002

[12] M. Lundberg, J. Eliasson, L. Svensson, P. Lindgren. "Context Aware Power Optimizations of Wireless Embedded Internet Systems". In Proceedings of IMTC 2004. To be published.