IMPLEMENTING SECURITY IN A WIRELESS NETWORK FOR THE PROVISION OF MEDICAL CARE IN EMERGENCY SITUATIONS

S. Dembeyiotis, G. Konnis, and D. Koutsouris

Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece

sdemb@biomed.ntua.gr konnis@biomed.ntua.gr dkoutsou@biomed.ntua.gr

Abstract: In the process of developing a wireless networking infrastructure to enable communications support for personnel involved in managing major emergency situations (earthquakes, floods, large-scale fires, etc) we are faced with the task of incorporating a robust data security mechanism, necessary since sensitive personal data (such as biosignals) will need to be handled confidentially. Links may be compromised, with an intruder being able to gain access to the data and extract sensitive information, such as personal medical files in the form of ECG exams, sonograms,, etc. We evaluated a number of design approaches, which had to satisfy the requirement of minimal operator intervention and automatic self-configuration of network nodes on startup. The final implementation allows for node control and management from remote network locations, while the nodes can transmit their data to other nearby network nodes securely, utilizing the latest commercially available cryptography solutions. Initial testing on our wireless testbed validates the design choices.

Introduction

The network consists of PC-based nodes which can be operated by non-technical personnel and can facilitate the transmission of IP-based data, including biomedical signals, images, video, voice, etc. The design differs from wireless network topologies which have been proposed for implementation in hospitals or individual mobile ambulance units [1] since the main network nodes are to operate unattended, scattered over the disaster area, and their function is to act as hubs for the connection of wireless sensors that can relay biosignals, and other data which are then made accessible over the network to any node. We selected IEEE 802.11 - based interfaces operating in the 2.4/5 GHz ISM bands [2]. The technology allows us to take advantage or recent implementations of very secure algorithms, which overcome earlier weak cryptography implementations. [3] In addition, the legacy sensor hardware was "IP-enabled" by using "device server" hardware, which encapsulates the serial port outputs into an IP stream and allows the sensors to be easily transported and connected to nodes around the network with little or no added complexity to network administration - compared to software driver based solutions.

A "device server" is a specialized network-based hardware device designed to perform a number of functions with client access independent of any operating system or proprietary protocol. The device allows the serial port of a legacy medical data generating sensor, such as a biosignal monitor, to become a networked node, meaning that the sensor acquires an IP address which uniquely identifies in a local or wider-area network and makes it accessible by all other IP-addressable network nodes. This allows much more flexibility than attaching a "terminal server" device to the sensor serial port, since this approach would still allow remote control but also present possible compatibility problems and offer limited management capabilities. In addition, extra hardware would be needed to implement the strong data security that is required. "Serial" type connections also have limited range compared to Ethernet-based ones, plus Ethernet protocols can monitor packet traffic losses and compensate, while "serial" technologies do not guarantee data integrity without the use of additional hardware and software.

Most importantly, encapsulating the "serial" data stream in an IP transport allows us to apply standards-based encryption and authentication policies. Encryption transforms data into secret code. An encryption algorithm employs a bit sequence ("key") to perform the necessary calculations. A larger a key makes it more difficult to break the code and retrieve the contents. A key allows the encrypted code to be decrypted or allows data to be encrypted. There are two types of keys used with data encryption-- secret keys and public keys. The two basic methods of encryption are symmetric and asymmetric, or public-key, encryption.

Symmetric (secret key) encryption uses the same key to encrypt and decrypt the data. Asymmetric (public key) encryption gives each party a pair of keys, a public key and a private key. Each party's public key is published while the private key is kept secret. Messages are encrypted using the recipient's public key and can only be decrypted using his private key, thus there is no needs for the two parties to share keys. In order to securely identify a party, a "digital certificate" policy can be employed. The most common algorithms used today in both encryption methods are DES, triple-DES and AES. DES (Data Encryption Standard) uses 64-bit keys for encryption, but only 56 bits for the data, and is no longer considered secure. Triple-DES uses three

ISSN: 1727-1983 © 2005 IFMBE

successive DES operations and provides far better security than DES, but it has been superseded by a new standard, AES, or Advanced Encryption Standard, which can use up to 256 bit keys. Starting in 2005, the US government will require NIST (National Institute of Standards and Technology) certified AES encryption as standard in all government organizations.

To initiate communication over unsecured channels, a software known as SSH (Secure Shell) is used. SSH can utilize many different encryption algorithms, including AES, to protect the data after the initial communication session is established. In addition to ensuring protection for the data stream, intruders should not be allowed to access and reconfigure a network device.

To protect wireless data streams over the chosen wireless technology, that is 802.11 a/b/g Wi-Fi, the most effective methods currently employed commercially are WPA (Wi-Fi Protected Access) and WPA2.[4] WPA uses a 128-bit encryption method known as TKIP (Temporal Key Integrity Protocol) while WPA2 uses 128 bit AES. Few commercial products support WPA2, but WPA has proven very hard to crack so far. For our design, where the network nodes need to self-configure, network with each other on startup and then continue to operate unattended, the most suitable crypto mode is WPA-PSK (Pre Shared Key) which allows for rekeying, that is automatic change of keys and authentication after a specified period of time, or after a specified number of packets have been transmitted. A "preshared" key is initially used, and then TKIP handles the encryption and automatic rekeying.

Materials and Methods

Our network design presents a rather complicated problem since it does not have a single point of data entry or exit, which can be protected by a software or hardware "firewall". The network nodes are interconnected, PC-based and run routing software which can utilize a number of routing protocols – data sensors are attached to these nodes via wireless or wired connections, and the data has to be protected both on the transmission path between the various sensors and the network node and throughout the network links. Here, we are concerned with the security of sensor data, mainly legacy medical devices with plain "serial" ports as their sole communications means, that have been network-enabled by the attachment of "device servers" which present the serial data stream encapsulated on a standard Ethernet port . The data are transmitted via cable to the Ethernet port of a nearby PC-based node, or wirelessly to a wireless device attached again to a similar node. The legacy sensors are now accessible over the network, but they have not become "smart" – they can operate either in an "always on" or in a polled mode. Since a legacy biosignal monitor, which provides patient ECG, Blood Pressure, Temperature and Pulse Oxymetry data over its serial port, now appears as an IP port to anyone on the network or beyond, a user can access the device server port and open a "tunnel" through which the serial data stream will arrive to his local Ethernet port, be extracted via a "port redirector" software utility and then presented to the appropriate viewing/analysis software as if the remote sensor was connected to a local "serial" port. That capability allows the use of existing viewing/analysis software, with no need for developing new "network-aware" versions. In a wired transmission situation, the data send over the wire to the network node are also encrypted, something that is not the case with standard "serial" port wire communications.

We evaluated a number of hardware products that are either commercially available as turn-key solutions or provide basic development platforms. We rejected the idea of developing our own encryption scheme using software crypto libraries since the market will increasingly demand products with NIST – certified encryption, and the certification process that is very costly and time-consuming and an option only for original equipment manufacturers. Companies like Lantronix and Digi offer a variety of NIST-certified server platforms, including some with embedded wireless capability. However, we decided to use separate wireless devices, not only for cost reasons but also due to the fact that commercial Wi-Fi products regularly receive updates for their firmware, including encryption capabilities, something that is not often the case with embedded industrial offerings.

On the software side, we developed a number of utilities that assist in the automatic network discovery and attachment after power-on, since the wireless devices we selected run Open Source Linux firmware, a feature that allows considerable customization. One example is the selection of WDS (Wireless Distribution System) transmit mode, which allows the legacy sensors to be connected in a peer-to-peer fashion and thus be available to any peer on the network. A software utility performs the necessary actions to automatically assign the proper IP address to every WDS bridging device that powers up, thus helping establish the link. On the PC-based network node side, we evaluated a number of software "port redirector" options which extract the serial data stream and make it appear as it is entering via a "serial" rather than an Ethernet port. The routing software that runs on every PC-based node can then re-route the data – in fact, the "IP encapsulated" data stream can be routed to any other node and appear as it is exiting from a "port redirector" locally.

Results

For testing, a device server was connected to a custom-made box which included a biosignal monitor with "serial" data output and the board of a Linux-based WLAN Access Point. The receiving side consisted of one of the network nodes, based on PC hardware, with a similar WLAN device connected to an Ethernet port and

ISSN: 1727-1983 © 2005 IFMBE

the appropriate software. A number of measurements were made to evaluate the performance of the wireless connection. When using video, we saw data rates over 25 Mbps with WPA-PSK on and utilizing 802.11g WLAN interfaces. We then manipulated the serial port on the biosignal monitor side, issuing command via the viewing software to select cetain ECG leads from a total of 12 available, and also set triggers for Blood Pressure alarms. The sensor side self-configured correctly on power-up and had no trouble initializing communication with the PC-based node side with the preshared keys. We used a number of Wi-Fi software "sniffers", which use various methods to break wireless encryption and extract the crypto keys, but WPA-PSK mode regenerated the keys too fast for the "sniffers" to crack the data stream security. In addition to testing with network-enabled legacy medical sensors, we also tested for successful transmission of audio with loseless compression – the signal being the output from an electronic stethoscope. The loseless codec data rates would stretch the capabilities of an asymmetric Bluetooth connection (one of the reasons we rejected Bluetooth technology as a wireless option) but caused no problems to the 802.11 data link, which under the very worst conditions still maintains a bidirectional bandwidth of 1 Mbps (half that if WDS mode is used). We also tested Voice over IP (VoIP) application performance by using a handheld PDA with VoIP software and WLAN capability. Audio performance was satisfactory while the hardware remained stationary, while jitter increased with mobility - a problem inherent in current WLAN implementations, which will be solved when Quality of Service (QoS) provisions are incorporated in upcoming IEEE 802.11 specifications. Our testing was limited to point-to-point connections before the wired/wireless medical or other sensors and a PC-based network node, since we have not yet implemented the routing software that would allow automatic routing under a number of scenarios, including node mobility.

Discussion

The initial results indicate that our approach succeeds in "network-enabling" legacy medical data sensors such as biosignal monitors, but also more multimedia-based sources such as the audio output from an electronic stethoscope, voice output from a VoIP phone used for commenting and audio/video from a monitoring camera which allows teleconsultation. The high bandwidth offered by 802.11 a/b/g technology allows for handling data bandwidths which are not possible with short-range wireless technologies such as Bluetooth. This because Wi-Fi at 2.4 and 5 GHz can offer from 1 to over 40 Megabits per second effective data rates, while Bluetooth can only offer 700 Kilobits per second (v1.2) Newer versions of Bluetooth promise rates in the low Megabits range, but they are slow to materialize commercialy. At the same time, innovations in antenna switching technology allow Wi-Fi to more than double ts effective range for a given data rate In addition, the results are obtained with the data being fully secured during transfer thanks to the WPA crypto mode featured by current Wi-Fi devices, which allows for dynamic key generation with no need for operator intervention. With ongoing firmware updates, today's WPA devices will soon offer WPA2 so NIST-certified security will be available for the wireless part of the network as well. Finally, for the "network enabled" scheme to be successfuly tested network-wide, the network routing algorithm needs to be finalized, so that performance can also be tested under mobility conditions. A number of algorithms are under consideration, with a lot of attention paid to the so-called "mesh" techologies (AODV, OLSR, etc ad-hoc protocols). These are extremely important for an application such as the one we envision, since individual network nodes can be plaed in rbitrary positions in the area of interest, establish ad-hoc connections to their nearest wireless node and maintain full network connectivity even when mobile. With present Wi-Fi technology, wireless nodes can be mobile and remain connected only if they are in the coverage range of an Access Point, Multiple Access Points (APs) cannot network so that their clients can "see" each other – but APs can be linked via bridging, using a technology such as WDS, which allows a node to act as both a both a bridge and a repeater – although a penalty in the form of reduction in effective bandwidth to half the nominal rate has to be paid. With wireless speeds near 50 Mbps this is no longer as big a problem as it was with 802.11b technology, and we are investigating some interim network topologies based on WDS node linking. The longer term solution will certainly be based on a true mobile ad hoc protocol such as OLSR (Optimized Link State Routing Protocol) which as a table-driven and proactive protocol, it exchanges topology information with other nodes of the network regularly. It is similar in some respects to the HIPERLAN MAC layer protocol, standardised by ETSI. Open Source implementations for both Linux and Windows OS are becoming more widespread and we plan to experiment with the technology when stable routing software becomes available.

Conclusions

In the process of implementing the design for a wireless network which can serve as the communications infrastructure for aiding the operations of rescue crews during major emergencies, we propose a scheme of IP-enabling legacy medical signal and other sensors in a way which would allow the sensors to operate unattended and to be remotely controlled from any network node. The sensors are connected to their nearest network node automatically on power-up, and they immediately receive IP addresses and establish secure links to facilitate the transmission of the sensitive data using the latest commercially available encryption

ISSN: 1727-1983 © 2005 IFMBE

technologies which apply to the automated and unattended operational scenario that we envision. The early results are very satisfactory, validating our initial design choices, and we plan to better integrate the concept in the overall system architecture by developing the appropriate routing algorithms to allow true peer-to-peer communications capabilities in a highly mobile network of quickly deployable portable wireless nodes which can in turn support network-enabled legacy medical and telemetry sensors and other data sources.

References

[1] **P**AVLOPOULOS **S**., **K**YRIACOU **E**., **B**ERLER **A**., **D**EMBEYIOTIS **S**., and **K**OUTSOURIS **D**. **(1998)**: **'A novel emergency telemedicine system based on wireless communication technology – AMBULANCE'**, *IEEE Trans. on Information Technology in Biomedicine*, **2**, p. 261-267

[2] Institution of Electrical and Electronic Engineers (IEEE), (1997) Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specification, LAN MAN Standards of the IEEE Computer Society, IEEE Standard 802.11.

[3] **B**ORISOV **N**., **G**OLDBERG **N**. and **W**AGNER **D**. **(2001):** 'Intercepting Mobile Communications: The Insecurity of 802.11', Proc. of the Mobicom 2001 , Rome, Italy 2001

[4] **H**IGGINS **T**. (2002): *WPA - Wireless Security for the rest of us.* [online]. Tomsnetworking.com. November 1, 2002. Available from: http://www.tomsnetworking.com/Sections-article35-page1.php

ISSN: 1727-1983 © 2005 IFMBE