Wireless/Mobile Network Security
Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. – - –


Chapter 17

# Security Issues in Wireless Sensor Networks used in Clinical Information Systems

Jelena Mišić and Vojislav B. Mišić
*Department of Computer Science*
*University of Manitoba*
*Winnipeg, Manitoba R3T 2N2*
*Canada*
E-mail: vmisic@cs.umanitoba.ca

**Abstract**

High quality healthcare environment is an important aspect of today's society. Areas such as diagnosis, surgery, intensive care and treatment and patient monitoring would greatly benefit from light untethered devices which can be unobtrusively mounted on patient's body and sense health variable. Those sensors have low power transceivers which can communicate to the interconnection device mounted on the patient's bed. Interconnection device should also have larger range wireless interface which should communicate to the access point in the patient's room, operation room or to the access points within the healthcare institution. Results of measurements of patient's health status will be stored in central medical database. The whole medical information systems is comprised of patient's personal sensor networks, department/room networks, hospital network and medical databases. Patient's privacy and integrity of personal health records must be protected within the whole clinical information system. In this chapter we address security and networking architecture of the clinical information systems with emphasis on the wireless hop which includes sensor networks and wireless local area or mesh networks. We review confidentiality and integrity polices for clinical information systems and discuss the feasible enforcement mechanisms over wireless hop. We also compare candidate technologies IEEE 802.15.1 and IEEE 802.15.4 from the aspect of resilience of MAC and physical layers to the jamming and denial-of-service attacks.

# 1 Introduction

Healthcare is important area for deployment of wireless sensor and personal area networks. The IEEE 1073 Medical Device Communications standards organization is currently in the process of developing of specifications for wireless interface communications. The main objective for this effort is to develop universal and interoperable devices for medical equipment which are transparent to the user, and easy re-configurable. The group has recognized that developing new wireless technologies is not an option and is looking instead in deployment of existing wireless technologies belonging to IEEE 802 family in the healthcare applications.

There are many research issues related to sensor and Wireless Personal Area (WPAN) networks in healthcare. First, there are different healthcare applications which monitor vital signs, electrocardiogram signals (ECG), electroencephalogram signals (EEG), dialysis devices, infusion devices etc. All these applications require some minimum event detection reliability i.e. minimum number of data bits per second as a result of sampling and digitizing analog health variables. Therefore, it is important to pair the medical application with low rate WPAN technology from the aspect of sufficient bandwidth as well as from the aspect of supported security mechanisms. It is not realistic to assume that a single WPAN technology can cope with requirements of different medical applications. Then, among the candidates for one application it is necessary to address several issues with equal importance:

1. We need to look into clinical information systems security policy of patient's medical record and protect the data's confidentiality and integrity from patient's WPAN's from the access of unauthorized personnel. It is necessary to develop secure sensor/WPAN/WLAN security and network architecture which can reliably and securely monitor health application on individual mobile patients without harming their health or life habits.

2. We need to look at secure location management when patient walks through the hospital or his/her bed is moved from room to room.

3. We need to look at the security issue of denial of service at the physical and MAC layers (jamming) which can cut the flow of patient's data to the monitoring station. This problem is related to the interference issues since every mobile patient or patient's bed presents independent

WPAN(s). They might interfere among themselves, and with WLAN running in the room or WPAN carried by the doctor/nurse.

4. We need to provide secure interconnections among different WPANs among themselves and with WLAN. The efficiency of interconnecting devices will determine the scalability of our secure healthcare network design.

5. The delay issue which is related to the Medium Access Control (MAC) protocol used in particular technology. It is also necessary to look at the packet size for given technology since all measured analog health variables after analog-to-digital conversion and encryption produce stream of bits with constant rate and packetization delay becomes an issue.

We start the chapter by reviewing the clinical information security policies. Then, we propose networking and security architecture of clinical information system which includes patient sensor networks, wireless local area networks which belong to the departments, and the central medical database where results of patient examinations are held. Enforcement of policy rules using cryptographic mechanisms over networking infrastructure is discussed, followed by a discussion of the classification of medical applications and pairing with WPAN technologies. We also compare some candidate technologies for wireless sensor networks from the aspects of MAC and physical layer security and sensing reliability. A brief summary concludes the chapter.

## 2 Security policy for healthcare sensor networks as part of clinical information systems

Sensor networks in medical applications are the edge component of the clinical information system. The wireless data flows with health variables measurements are part of "personal health information" and must be protected in the aspects of integrity and patient's privacy before they are stored in the patient's "medical record". Actually, health sensing information is a part of the medical record. The security policy for medical records has been carefully designed in order to limit the number of clinicians who can access the patient's record and to control the operations over the record [2, 4] and can be expressed as the number of rules, as follows:

1. Each medical record has an access control list naming the individuals and groups who may read and append the information to the record.

The system must restrict the access to those identified on the access control list.

2. One of the clinicians on the access control list (called the *responsible clinician*) must have right to add other clinicians to the access control list.

3. The responsible clinician must notify the patient of the names on the access control list whenever the patient's medical record is opened.

4. The name of the clinician, the date, and the time of the access of a medical record must be recorded.

The purpose of previous four access rules is to control the confidentiality of the medical record. Patient must consent to the treatment and he/she must have the access to his/her record at any time and be informed whenever any clinician accesses the record.

Integrity of the patient's medical record is protected by the following set of rules:

**Creation** When new medical record is created the clinician creating the record should have access as should the patient. If the medical record is created due to the referral from another referring clinician he/she should also have the right to access the medical record.

**Deletion** Clinical information cannot be deleted from medical record until the appropriate time has passed.

**Confinement** Information from one medical record may be appended to a different medical record if and only if the access control list of the second record is a subset of the access control list of the first.

**Aggregation** Aggregation of patient data must be prevented.

**Enforcement** Any computer system that handles medical records must have a subsystem that enforces previous rules.

Existence of wireless sensor networks integrated in medical information systems puts a big challenge on the implementation of aforementioned rules. Unfortunately, previous access principles can not be implemented as access lists in the network. Instead, we will need to use some cryptographic techniques which we will discuss in the next section.

# 3 Security architecture of wireless part of medical information system

Let us consider the medical information system infrastructure including wireless sensor networks as shown in Fig. 1. Important parts of the architecture are patient's security processor which is attached to bed and patient's room wireless access point. Patient's security processor is module with both security and networking functions. From security aspect it generates the symmetric encryption key by which all data packet with sensed health information are encrypted. It distributes the symmetric key to the sensing nodes by encrypting it with public key which is common for all sensing nodes. Sensing nodes are pre-configured with the private key by which they can decrypt the symmetric key. Sensing nodes will send packets with encrypted payload and completely authenticated to the patient's security processor (PSP) which further forwards after possible aggregation to the room's access point.

From the networking aspect, PSP is the coordinator of sensing nodes which belong to the patient's Personal Area Network (PAN) and participates in the Medium Access Control function of the nodes. For example, for IEEE 802.15.1 technology (Bluetooth) PSP will be executed on the piconet's master and for IEEE 802.15.4 PSP will be executed on the cluster's coordinator.

Access point is further connected to the central medical record database through computer network and forwards encrypted and authenticated packets to the central database. Data packets which carry measurements of personal health variables must be authenticated and encrypted in the way which we discuss below. From the networking point of view access point is interconnection device which interconnects Personal Area Network technology (IEEE 802.15.1 or IEEE 802.15.4) with hospital's network which is might be implemented using wireless LAN and mesh technologies.

Medical personnel might carry their own PAN nodes and communicate directly to medical health database through the patient's room access point.

Security of medical applications over sensor networks has to be protected at every networking layer. At the physical and MAC layer there exists possibility of denial of service attack by generating to much interference or by generating unnecessary traffic. Therefore, MACs should be evaluated from this perspective also. Payload of packets with sensed data should be encrypted when needed. Also, in some situations, patient's location should be hidden as well. Given the hierarchical application architecture, there

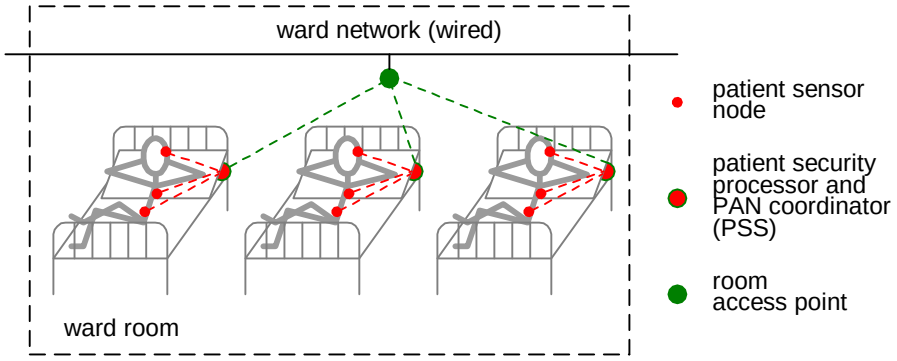


Figure 1: Security architecture of wireless part of medical information systems

should exist layered security architecture with different keys and possibly different encryption algorithms at WPAN, room and hospital level. The encryption standards used at particular level should match importance and vulnerability of the data. For example the traffic at the WPAN level has to be encrypted at the MAC level but the traffic between access points should be protected by IPSec.

However, security measures will affect the delay and throughput of sensed health data and this impact has to be carefully evaluated. Initial work on performance evaluation of IPSec is presented in [9] but much more needs to be done for multi-tier communication architecture built over WPANs. We plan to develop multi-layer security architecture which will match confidentiality and integrity of the sensed data and evaluate the performance of overall application architecture.

## 4 Enforcement of privacy and integrity rules

In order to protect from the attacks from the outside world, all hospital equipment and personnel must possess the secret 'hospital/department/room' key $K_H$. This key is used to sign and authenticate network packets generated by the equipment and personnel belonging to specific medical department. Authentication is achieved by calculating the hash function over the packet with measurement data, hospital/department/room key and timestamp $T_s$ with time of packet generation. For hash function, we adopt Secure Hash Algorithm (SHA) [27]. Let us denote $i$-th packet containing measurements

of some health variable as $P_i$, its Medium Access Control header as $H_i$ and its payload as $D_i$. Packet authentication code for packet $i$($\text{PAC}_i$) can then be calculated as

$$PAC_i = H(K_H, T_{s,i}, H_i||D_i).$$

### 4.1 Patient's privacy

Aforementioned access policy rules require that only patient and clinicians have access to patient's medical record and that patient must be informed of any access to his/her record. Therefore, this small group must have dedicated secret session key $K_p$ (p comes from patient who is the principal of the group), but no one from this group must have the capability to derive the key without the participation of other members. Particularly, participation of the patient is necessary in all accesses. This key will be used as encryption key of an symmetric encryption system such as 3-DES (Data Encryption Standard) or AES (Advanced Encryption Standard). Operations of encryption and decryption with patient's key will be denoted as $E_{K_p}()$ and $D_{K_p}()$ respectively. Encryption using public key cryptography takes long time and generates high packet payload which is a problem for existing candidate technologies for wireless sensor networking.

Process of generating patient's key requires attention. If the patient is unable to participate in the decisions regarding his/her healthcare, then his part of the key generation must be done either by proxy person or by central hospital authority. Clinicians who are supposed to participate in the key generation are responsible (principal) clinician and referring clinician. Therefore we assume that minimum three entities must participate in the generation of patient's key.

One approach which we adopted for patient's key generation is the concept of secret sharing with threshold. Secret is divided into $n$ parts called shadows and in order to recover it, $m$ shadows are needed. This idea was first independently proposed in [28] and [5]. It was further elaborated in [3, 18] and nice overview of the work in this area is given in [29].

Priority among the users can be modeled by giving important user more shadows. For example, for emergency cases central hospital authority together with responsible (principal) clinician should be able to reconstruct the patient's key. The basic mathematical idea behind the key generation among $m$ entities is to create the system of $m$ equations with $m$ variables by using the polynomial with random coefficients. For example for $m = 3$ we start from the polynomial:

$$F(x) = (ax^2 + bx + K_p) \bmod p$$

where $p$ is public random prime number, $a, b < p$ are secret random numbers and $K_p$ is patient's symmetric key. Assume that each participant $j$ in key generation has some numerical representation of his/her identity $ID_j$. Then shadows become

$$\begin{array}{lcll} F(ID_{pt}) & = & (aID_{pt}^2 + bID_{pt} + K_p) \bmod p & \text{patient's shadow} \\ F(ID_{pc}) & = & (aID_{pc}^2 + bID_{pc} + K_p) \bmod p & \text{principal clinician's shadow} \\ F(ID_{rc}) & = & (aID_{rc}^2 + bID_{rc} + K_p) \bmod p & \text{referring clinician's shadow} \\ F(ID_{ca}) & = & (aID_{ca}^2 + bID_{ca} + K_p) \bmod p & \text{central authority's shadow} \end{array}$$

To generate the patient's key and start the measurement of health variables, three shadows are needed and must be presented to PSP. For the start of measurement, patient's shadow, principal clinician's shadow and central authority's shadow are sufficient. Three shadows are also needed in order to decrypt the medical record from the medical database which is also encrypted with $K_p$. In this case, central authority should be excluded and key should be recovered from patient's shadow, principal clinician's shadow and referring clinician's shadow. In this case, patient will be always notified when his/her record is accessed and he/she will be sure that record is not changed. Shadows should be changed frequently.

### 4.2 Timestamping the sensed records as results of patient's examination

The fourth access rule calls for recording of all accesses for the purpose of auditing. Auditing requires that accesses are recorded together with the date, time and name of each person who accessed the record. This problem can be solved by linking current record of access (timestamp, list of persons involved) with previous records as proposed in [19, 20, 21, 29, 4]. It is also facilitated by the fact the central medical database can be associated with the trusted timestamping server. Server builds a tree of hashes of timestamping requests received for given time period (second, minute). Server further sends to the medical database signed hashes from the leaf generated by the opening of patient's record till the root of the tree. Assume that information about patient's $i$ record is $n$-th leaf in the tree counting from the root and it has format:

$$R_{ID_{pt},n} = T_n, L_n, K_p, ID_{pc}, ID_{rc}.$$

where $L_n$ denotes the record lifetime. Let us denote $H_n = H(R_{ID_{pt},n})$. Let us also assume that timestamping server has public/private key pair $K_t$

and that encryption with public and private key is denoted as $V_{K_t}$ and $S_{K_t}$ respectively. Then timestamping server will associate information about access to the patient's record with:

$$S_{K_t}H((H_0, H_1, H_2...H_n)).$$

where $H_0$ represents the hash of the information at the root of the tree and $H_i$ are hashes of the access information along the path to the root of the tree.

Timestamping is also related to the deletion principle which states how long patient's medical record must be kept before deletion. The lifetime of the patient's examination record $L_n$ which is entered into medical database must be also protected using the timestamping service. Patient's record lifetime can be determined staring from the moment when record is generated. If the particular record is missing but its hash exists in the timestamping tree, the integrity of the patient's record is corrupted.

### 4.3 Enforcement of the confinement principle

Patient must be informed when clinician non-familiar to his/her medical record accesses the record. On the other hand responsible clinician must be able to add other clinicians to the access list. In that case the number of secret shadows has to change (increase) and central clinical authority has to increase the number random parameters in the equation which determines secret shadows. For example, if second clinician has to be added to the access list, the system of secret shadow equations becomes:

$$\begin{array}{lcll} F(ID_{pt}) & = & (aID_{pt}^3 + bID_{pt}^2 + cID_{pt} + K_p) \bmod p & \text{patient's shadow} \\ F(ID_{pc}) & = & (aID_{pc}^3 + bID_{pc}^2 + cID_{pc} + K_p) \bmod p & \text{principal clinician's shadow} \\ F(ID_{sc}) & = & (aID_{sc}^3 + bID_{sc}^2 + cID_{sc} + K_p) \bmod p & \text{second clinician's shadow} \\ F(ID_{rc}) & = & (aID_{rc}^3 + bID_{rc}^2 + bID_{rc} + K_p) \bmod p & \text{referring clinician's shadow} \\ F(ID_{ca}) & = & (aID_{ca}^3 + bID_{ca}^2 + bID_{ca} + K_p) \bmod p & \text{central authority's shadow} \end{array}$$

In this case four out of five shadows are needed to generate or access the patient's examination record so this presents (4,5)-threshold scheme.

### 4.4 Enforcement of the aggregation principle

Aggregation of patients' records must be prevented in the case the principal/second clinician becomes corrupted. This is mostly prevented by sharing the secret encryption key through the shadows. Another helpful thing would

be to encrypt the database records [11, 10]. The index filed can be the hash of last name of the patient concatenated with his/her ID number. Data fields must be encrypted by the secret key assembled from $m$ secret shadows. In this way, the list of the patients is hidden as well as their medical records.

# 5 Impact of the wireless PAN technologies

We plan to evaluate current WPAN standards namely, IEEE 802.15.1, and 802.15.4 and their interworking among themselves and with IEEE 802.11b WLANs as major candidates for implementations of healthcare sensor networks. We agree with [7] that the success of wireless sensor networks as a technology rests on the success of the standardization efforts to unify the market and avoiding the proliferation of proprietary, incompatible protocols that, although, perhaps optimal in their individual market niches, will limit the size of overall wireless sensor market.

## 5.1 Classification of healthcare applications and pairing with WPAN technologies

We will analyze a number of healthcare applications from the aspects of bandwidth and delay. For example electrical signals from the heart are sampled at the rate of 500 samples per second and each sample is digitized to 8 bits giving data flow of 4000bps. Furthermore, samples must be taken from several points on the body. Each flow can not be delayed more than few hundreds of milliseconds and flows must be synchronized. We will look at the following issues which are of foremost importance for sensor networks and which follow from the requirement for controlled event detection reliability at the network sink and use them as criteria to match the technology with the application.

1. How much is physical layer immune to the interference errors? We note that all candidate technologies run in Industrial Scientific and Medical (ISM) band between 2400 and 2483.5MHz. They use different modulations at the physical layer, for example 802.15.4 and 802.11 use Direct Sequence Spread Spectrum (DSSS) and 802.15.1 uses Frequency Hopping Spread Spectrum. Therefore dynamic channel allocation algorithms and interference mitigation techniques will be needed to avoid excessive interference at the physical layer. Some work on interference mitigation between 802.151 and 802.11b is reported in

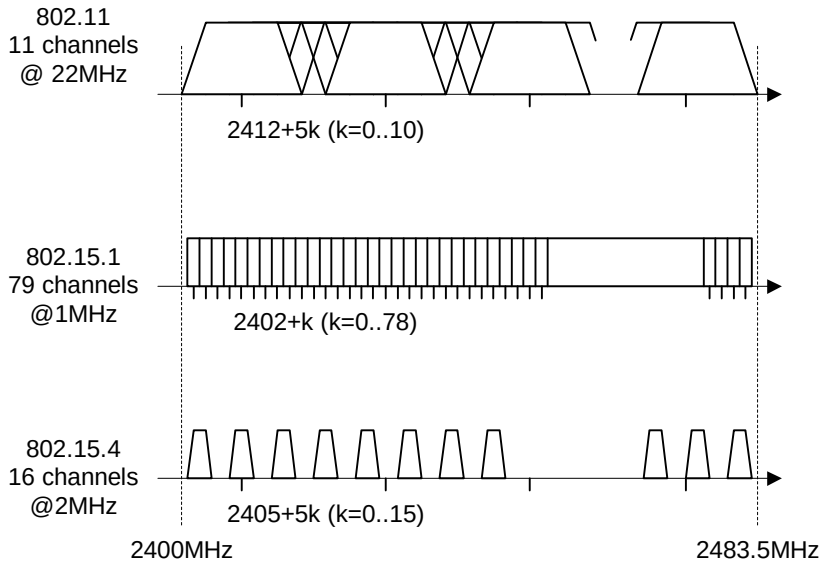


Figure 2: Spectrum usage for various WPAN technologies running in ISM

[14] but much more is needed for the interworking with 802.15.4. The channel layout for all the technologies under consideration is given in Fig. 2.

2. The MACs for candidate technologies can be classified as TDMA with polling and CSMA-CA. Node access delay has to be evaluated for both MAC classes under varying number of nodes and packet rate from node. Is acknowledged transfer necessary for achieving desired event reliability and which packet spacing it induces? How much of the buffering is reasonable to have at the source nodes? For specific MAC, maximum effective bandwidth left to the application has to be evaluated and paired with the delay.

### 5.2 Design and evaluation of interconnection devices

There will be a need to interconnect different WPAN and to interconnect WPAN/WLAN networks in order to regulate the scale of power, distance, and bandwidth-related issues. The example of location of interconnecting devices (bridges) is given in Fig. 1.

These devices have to be designed in the scope of MAC, channel and buffering issues and their performance has to be evaluated. The operation

of interconnection device is very important for the overall network design since it affects the end-to-end delay and the scalability of the overall design. Some work in this area exists for interconnection of Bluetooth piconets. The work in [32, 31] requires computation of non-overlapping rendezvous points for bridges while the work in [25] allows bridge to visit the piconet at will trading delay for scalability. However, little is known about interconnections between IEEE 802.15.4 with other WPANs and WLANs.

### 5.3 Reliable event detection

The rate at which data is propagated from source nodes at patient's body to monitoring devices at the patient's bed and monitoring room (sink) must be high enough to obtain the desired event detection reliability $R$, which is commonly defined as the number of data packets required per second for reliable event detection at the sink [1]. At the same time, sensor nodes operate on battery power which means that energy efficiency must be maintained.

Reliable event detection using minimal energy resources requires simultaneous achievement of several sub-goals. First, packet loss along the path from source to the sink has to be minimized; at the Physical (PHY) layer, packets can be lost due to noise and interference, while at the Medium Access Control layer (MAC) layer, losses may be incurred by collisions. Second, packet waiting has to be minimized, including queueing delays experienced in various devices along the data path towards the sink, but also delays due to potential congestion in the network. Congestion control has to be addressed as a cross-layer problem and solved at the MAC level since excessive active nodes have to be turned off [23]. Finally, packet propagation should take place along the shortest paths, while avoiding congested nodes and paths; this is the responsibility of the network layer.

Given that the protocol stack on sensor nodes—which are battery-operated and have limited computational capabilities—has to be as simple as possible, we conclude that simultaneous minimization of packet losses and improvement in efficiency (with the goal of maximizing the lifetime of the network) necessitate that some of the aforementioned functions of different layers are performed together. In other words, cross-layer optimization of network protocol operation is needed; the feasibility of this optimization is determined by the communication technology used to implement the network. This problem has classically been treated only as a graph-theoretical problem where only connectivity has been addressed [30, 15] or addresses the collision based MAC [8] although it does not allow the active node to get into the sleep state and achieve load balancing among the nodes. Second group of

proposals [17, 12] tries to regulate the event sensing reliability but without looking at MAC and PHY properties at all. The congestion problem is particularly important in networks which use a collision-based MAC protocol such as CSMA-CA, e.g., in 802.15.4 [16]. The decrease in throughput due to congestion may lead the coordinator to the erroneous conclusion that the number of active nodes is too low. Therefore it is important to look at the cross-layer implementation of power/congestion control in wireless sensor networks.

### 5.4 Handling patient's mobility

The patient wearing wireless sensors will either walk within the hospital or he will lie in his bed while the bed is moved to another room. Therefore, sensed data will have to be sent to new access points and experience new level of interference and congestion. The handover procedure can be handled at the MAC layer or at the networks layer. The handover between 802.11 MACs is analyzed in [22]. However there is an open issue about how the handover between 802.15.4 and 802.11 or between 802.15.1 and 802.11 has to be executed, and how much of data flow interruption will occur. We plan to design and analyze secure MAC layer handover procedures between involved WPAN and WLAN technologies.

Besides MAC layer handover, it can happen that network layer handover is also needed if the IP subnets covering access points have changed. Once when MAC layer handover is finished, the mobile node (bridge on the patient's bed) has to discover the network layer information on the link, i.e. the new care-of-address router and network prefix. Foreign routers periodically advertise this in Router Advertisement using mobile IPv6. When mobile node learns the new care-of-address it registers this address with its home agent. We have to model and evaluate the acceptability of latencies and packet losses during secure network layer handover.

## 6 Comparison between two technologies regarding the deployment in sensor networks

After individual descriptions of IEEE 802.15.1 and IEEE 802.15.4 we will give direct comparison of their properties against the criterion of feasibility of their deployment in sensor networks.

### 6.1 How much is physical layer immune to the noise errors

Both standards, 802.15.1 and 802.15.4 with 250kbps rate, operate in 2450MHz band known as Industrial, Scientific and Medical – ISM. This band is already hosting wireless LAN/PAN standards such as 802.11b and 802.15.1 (Bluetooth) and a lot of interference is expected. It is also worth mentioning that Bluetooth packets can be 1, 3 or 5 slots long which results in payload sizes of 17, 121, 224 bytes for DM 1, 3 and 5 packet types respectively with Forward Error Correction (FEC) or in payload sizes of 27, 183 and 339 bytes for DH-type , 1, 3 and 5 packet types without FEC. On the other hand, 802.15.4 does not have FEC and allows maximum packet size of 127 bytes. This packet size includes all headers from physical and MAC layer which minimum size is 15 bytes giving the actual maximum payload size of 112 bytes. Therefore, it makes sense to compare these two technologies only in the case of payload size of 27 bytes (DH1).

As mentioned, Bluetooth uses FHSS and is very resilient to interference. According to the exhaustive simulation results reported in [33] when 10 fully loaded piconets each with 7 slaves are placed in the room with dimensions 10m x 20m, (and interfere with each other) packet error rate for DH1 packets was 0.03. When the same experiment was repeated with 100 co-located piconets, packet error rate was 0.3.

IEEE 802.15.4 standard in the 2450 MHz range (ISM band) uses 16-ary quasi-orthogonal modulation technique. Four data bits represent one modulation symbol and that symbol is further encoded into 32 bit chip sequence. There are 16 nearly-orthogonal Pseudo-Noise chip sequences. Each chip sequence is modulated onto the carrier using offset quadrature phase shift keying (O-QPSK). Since the chip rate is 2Mcps and raw data rate is 250kbps the maximum supported ratio of bit energy to the noise power spectral density of $\frac{E_b}{N_0} = 8$. According to the properties of QPSK, the Bit Error Rate is determined using known expression given for example in [13]. Therefore, without the interference, we should expect BER slightly less than $10^{-4}$. This is confirmed in the section 6.1.6 of the standard where Packet Error Rate (PER) of 1% is expected on packets which have 20 bytes including MAC and physical level headers. However, in the presence of interference in the ISM band, it is more realistic to expect BER around $10^{-3}$ and Packet Error Rate more than 28% for packets with 27 bytes of payload and 15 bytes of headers. (Packet Error Rate can be calculated as $PER = 1 - (1 - BER)^X$ where $X$ is packet length including MAC and physical layer header expressed in bits).

Although, Zürbes' experiment can not be directly translated into BER,

10 co-located piconets present interference probably much larger than what the physical layer of 802.15.4 can handle.

## 6.2 The access delay

Bluetooth has a polling based MAC protocol and its access delay depends on the order in which master polls the slaves and on the amount of packets which are exchanged between master and slave in one visit. Mathematically speaking, packet service time directly depends on the piconet cycle time i.e. the time needed for the master to visit each slave. It has been shown [26] that under low traffic exhaustive scheduling (where master exchanges packets with slave as long as one of them has packets in the queue) offers the lowest access delay compared with other limited round-robin polices where master can exchange at most $M$ packets per one polling cycle. However, under high loads exhaustive scheduling is not the best one compared to limited polices and fairness issue raises since one station can keep the master busy for a long period of time. Under limited policies every station has equal amount of bandwidth and piconet cycle time is limited. Therefore, if one or more slaves have excessive traffic their packets will suffer from the large delay, but the other slaves with lower traffic will not.

## 6.3 Can wireless sensor network reach the regime when delays are unacceptable?

Bluetooth piconet can reach such regime only if duration of piconet cycle becomes extremely long and this can happen only under exhaustive scheduling of slaves. This can represent also a security problem, since one malicious node can bring the whole piconet down.

IEEE 802.15.4 network can reach this saturation regime if the number of nodes and packet arrival rates exceeds certain limits. For example, for packet size of 30 bytes (including PHY and MAC headers) saturation is reached with 30 nodes each having packet arrival rate of 3 packets per second (total of 45 bytes per second). Under packet size of 90 bytes, saturation is reached with 15 nodes with packet arrival rate of 3 packets per second. Saturation also can represent a security problem since a couple of malicious nodes can quickly bring the network down as shown in [24].

### 6.4 How much of the buffering is reasonable to have at the source nodes?

Assuming that whole sensing measurement can be stored in one packet, transmitting several packets from the node's buffer means that some slightly older information is sent. Also, the inter-packet time will be less than in the case where each node sends one packet only. Therefore, exhaustive scheduling of active sensor's periods with large buffers increases spatial and temporal correlation of sensed data. This fact is important in the applications where controlled reliability means controlled inter-packet spacing or in applications with security concerns where mal-functioning node with exhaustive scheduling can inject large amount of bogus data into the network. Therefore, buffer sizes at the nodes should not exceed several packet sizes.

### 6.5 What is the effective bandwidth left to the application, i.e. what is the maximum possible event detection reliability for particular MAC?

The concern in sensor network applications of Bluetooth is that downlink packet slots will be empty and that maximum throughput of the network in that case can be at most 723kbps out of 1Mbps in Bluetooth version 1.2 with DH5 packets. The recent Enhanced Data Rate option in Bluetooth version 2.0 allows for maximum data rates over 2Mbps [6].

On the other hand, IEEE 802.15.4 has maximum raw data rate of 250kbps i.e. four times less than Bluetooth and CSMA-CA MAC protocol. Due to the backoff procedure and listening to the medium, the traffic intensity of one node affects the activities of the others. Under large traffic which can originate from many nodes, there will be many collisions and many deferred transmissions. This results in severe congestion and all nodes experience large delays. In such situation which is termed as saturation, throughput drops to few percent of the raw data rate. Since in IEEE 802.15.4 backoff window can not exceed value of 31 and packet size is limited to 127, network can easily reach the saturation regime. Our results show that highest throughput of 25% occurs for packet size of 90 bytes (including PHY and MAC headers), 5 active stations in the network (we did not check for smaller number station) under superframe size of 48 backoff periods. This puts a limit of effective data rate of 62.5 kbps per cluster, or around 12.5 kbps per node. However, under 15 active nodes the total throughput drops to 18% and this drop continues with the increase of the cluster size.

## 7 Summary

In this chapter we have addressed security and networking architecture of the clinical information systems with emphasis on the wireless hop. Wireless hop includes sensor networks and possibly wireless local area or mesh networks. We have reviewed confidentiality and integrity polices for clinical information systems and proposed the policy enforcement mechanisms which cover the wireless hop. We have compared candidate technologies IEEE 802.15.1 and IEEE 802.15.4 from the aspect of resilience of MAC and physical layers to the jamming and denial-of-service attacks.

## References


[1] O. B. Akan and I. F. Akyildiz. ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks. In *IEEE/ACM Transaction on Networking (to appear)*, October 2005.

[2] R. Anderson. A security policy model for clinical information systems. In *Proc. of the 1996 IEEE Symposium on Security and Privacy*, pages 34–48, 1996.

[3] C. Asmuth and J. Bloom. A modular approach to key safeguarding. *it*, 29(2):208–210, 1979.

[4] M. Bishop. *Computer Security – Art and Science*. Pearson Education, Inc., Boston, MA 02116, 1st edition, 2003.

[5] G. R. Blakely. Safeguarding cryptographic keys. In *Proceedings of the National Computer Conference, American Federation of Information Processing Societies*, volume 48, pages 313–317, 1979.

[6] Bluetooth SIG. *Draft Specification of the Bluetooth System*. Version 2.0, Nov. 2004.

[7] E. H. Callaway, Jr. *Wireless Sensor Networks, Architecture and Protocols*. Auerbach Publications, Boca Raton, FL, 2004.

[8] A. Cerpa and D. Estrin. Adaptive self-configuring sensor network topologies. In *Proceedings Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies IEEE INFOCOM 2002*, volume 3, pages 1278–1287, New York, NY, June 2002.

[9] O. Elkeelany, M. M. Matalgah, K. P. Sheikh, M. Thaker, G. Choudry, D. Medhi, and J. Qaddour. Performance analysis of IPSec protocol: Encryption and authentication. In *Proceedings of IEEE International Conference on Communications ICC 2002*, pages 1164–1168, 2002.

[10] J. Feigenbaum, M. Liberman, and E. Grosse. Cryptographic protection of mebership lists. *Newsletter of the International Association of Cryptologic Reserach*, 9:16–20, 1992.

[11] J. Feigenbaum, M. Liberman, and R. N. Wright. Cryptographic protection of databases and software. *Distributed Computing and Cryptography, J. Feigenbaum and M. Merritt eds.*, pages 161–172, 1991.

[12] J. Frolik. QoS control for random access wireless sensor networks. In *Proc. WCNC 2004*, Atlanta, GA, Mar. 2004.

[13] V. K. Garg, K. Smolik, and J. E. Wilkes. *Applications of CDMA in Wirless/Personal Communications*. Prentice Hall, Upper Saddle River, NJ, 1998.

[14] N. Golmie. Bluetooth dynamic scheduling and interference mitigation. *ACM/Kluwer Journal on Special Topics in Mobile Networking and Applications (MONET)*, 9(1):21–31, 2004.

[15] H. Gupta, S. Das, and Q. Gu. Connected sensor cover: self organization of sensor networks for efficient query execution. In *Proceedings 2003 ACM International Symposium on Mobile ad hoc networking & computing*, volume 1, pages 189–200, Annapolis, MD, June 2003.

[16] Standard for part 15.4: Wireless MAC and PHY specifications for low rate WPAN. IEEE Std 802.15.4, IEEE, New York, NY, Oct. 2003.

[17] R. Iyer and L. Kleinrock. QoS control for sensor networks. In *Proc. ICC'03*, volume 1, pages 517–521, Anchorage, AK, May 2003.

[18] E. D. Karnin, J. W. Greene, and M. E. Hellman. On sharing secret systems. *it*, 29(2):35–41, 1983.

[19] R. Merkle. Method of providing digital signatures, Jan. 1982.

[20] R. Merkle. A digital signature based on a convnetioanl encryption function. In *Proceedings of the Advances in Cryptology - CRYPTO'87*, pages 369–378, 1988.

[21] R. Merkle. A certified digital signature. In *Proceedings of the Advances in Cryptology - CRYPTO '88*, pages 218–238, 1990.

[22] A. Mishra, M. Shin, and W. Arbaugh. An empirical analysis of the ieee 802.11 mac layer handoff process. *SIGCOMM Comput. Commun.*, 33(3):93–102, 2003.

[23] J. Mišić, G. R. Reddy, and V. B. Mišić. Activity Scheduling based on cross layer information in Bluetooth sensor networks. *Computer Communications*, to appear, 2006.

[24] V. B. Mišić, J. Fung, and J. Mišić. Mac layer security of 802.15.4-compliant networks. In *Proc. WSNS'05, held in conjunction with IEEE MASS05 2005*, Washington, DC, Dec. 2005.

[25] V. B. Mišić, J. Mišić, and K. L. Chan. Walk-in scheduling in Bluetooth scatternets. *Cluster Computing*, 8(2/3):197–210, 2005.

[26] Mišić, J. and Mišić, V. B. *Performance Modeling and Analysis of Bluetooth Networks: Network Formation, Polling, Scheduling, and Traffic Control*. Boca Raton, FL: CRC Press, July 2005.

[27] N. I. of Standards and T. NIST. *Digital Signature Standard*. US Deprtment of Commerce, 1994.

[28] A. Samir. How to share a secret. *IEEE Computer*, 22(11):612–613, 1979.

[29] B. Schneier. *Applied Cryptography*. John Wiley & Sons, Inc., New York, N.Y., 2nd edition, 1996.

[30] C. Schurgers, V. Tsiatis, S. Ganeriwal, and M. Srivastava. Topology management for sensor networks: exploiting latency and density. In *Proceedings 2002 ACM International Symposium on Mobile ad hoc networking & computing*, volume 1, pages 135–145, Lausanne, Switzerland, June 2002.

[31] G. Tan and J. Guttag. A locally coordinated scatternet scheduling algorithm. In *Proceedings of the 26th Annual Conference on Local Computer Networks LCN 2002*, pages 293–303, Tampa, FL, Nov. 2002.

[32] W. Zhang and G. Cao. A flexible scatternet-wide scheduling algorithm for Bluetooth networks. In *Proc. 21st IEEE International Performance, Computing, and Communications Conference IPCCC 2002*, Phoenix, AZ, Apr. 2002.

[33] S. Zürbes. Considerations on link and system throughput of Bluetooth networks. In *Proceedings of the 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC 2000*, volume 2, pages 1315–1319, London, UK, Sept. 2000.