Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2008, Article ID 291365, 18 pages
doi:10.1155/2008/291365

Research Article

Secure and Efficient Data Transmission over Body Sensor and Wireless Networks

Narasimha Challa, Hasan Çam, and Madhur Sikri

Computer Science and Engineering Department, Arizona State University, Tempe, Az 85287, USA

Correspondence should be addressed to Hasan Çam, hasan.cam@asu.edu

Received 16 June 2007; Revised 4 December 2007; Accepted 20 February 2008

Recommended by Yang Xiao

This paper addresses the transmission of medical and context-aware data from mobile patients to healthcare centers over heterogeneous wireless networks. A handheld device, called personal wireless hub (PWH), of each mobile patient first gathers and aggregates the vital sign and context-aware data for various telemedicine applications. PWH transmits the aggregated data to the remote healthcare center over multiple wireless interfaces such as cellular, WLAN, and WiMAX. The aggregated data contain both periodic data and those nonperiodic unpredictable emergency messages that are sporadic and delayintolerant. This paper addresses the problem of providing QoS (e.g., minimum delay, sufficient data rate, acceptable blocking, and/or dropping rate) by designing a packet scheduling and channel/network allocation algorithm over wireless networks. The proposed resource-efficient QoS mechanism is simple and collaborates with an adaptive security algorithm. The QoS and security are achieved mainly with the collaboration of differentiator, delay monitor, data classifier, and scheduler modules within the PWH. This paper also discusses secure data transmission over body sensor networks by introducing key establishment and management algorithms. Simulation results show that the proposed framework achieves low-blocking probability, meets delay requirements, and provides energy-efficient secure communication for the combination of vital signs and context-aware data.

1. INTRODUCTION

Future generation wireless networks are expected to experience huge demands from mobile telemedicine applications. Mobile telemedicine allows patients to do their daily activities while they are monitored continuously anytime, anywhere. Typical telemedicine applications include transmission of electro-cardiogram (ECG) signals from a mobile patient to a doctor, voice conversation between the doctor and the personnel in the emergency vehicle, transmission of X-rays, live video, and medical images from the emergency vehicle or the patient to the doctor at the healthcare center. These applications require communication between a mobile patient and a healthcare center. Further, these telemedicine applications have different QoS requirements that are specified in terms of the desired loss rate, delay, and bandwidth. Table 1 shows the typical telemedicine applications and their QoS requirements [1]. Mobile telemedicine applications will have to deal with the characteristics of wireless networks such as low bandwidth, channel fluctuations, and coverage changes. In addition, a single network alone may not be able to meet the bandwidth requirements of applications at all locations. In this paper, the mobile applications are enabled to take advantage of both the coverage and bandwidth provided by different wireless networks through multiple wireless interfaces in achieving their QoS objectives.

An important characteristic of telemedicine data is the difference in the periodicity and sporadic nature of the data. When a patient is under good conditions, the vital sign data of the patient are sent periodically to healthcare center to monitor the condition of the patient. The periodic data may consist of images, video, or audio. The exact constituents of the periodic data are specified by the doctor based on the patient's condition. When the patient's condition deteriorates, sporadic emergency data need to be sent to the healthcare center. The sporadic emergency data may be required to transmit high-bandwidth images. Wireless bandwidth can be reserved for periodic data because its amount and occurrence

Table 1: QoS requirements.

Services	Stream characteristic	Delay sensitivity	Data rate	Delay	Packet loss
Voice	Continuous	Delay sensitive	4–25 kbps	150–400 ms	3%
Diagnostic audio	Continuous	Delay sensitive	32–256 kbps	100–300 ms	1%
Video (normal quality)	Continuous	Delay sensitive	64 kbps–2 Mbps	150–400 ms	—
Voice (high quality)	Continuous	Delay sensitive	3–15 Mbps	100–300 ms	—
Signs (ECG)	Continuous	Delay sensitive	24 kbps/12 channels	—	—
Signs (heart rate)	Continuous	Delay sensitive	2–5 kbps	1s	—
Signs (blood pressure)	Continuous	Delay sensitive	2–5 kbps	—	—
Images (uncompressed)	Bursty	Delay insensitive	30–40 Mb	—	—
Images (regional)	Continuous	Delay insensitive	10–20 Mb	—	—

time can be determined. However, reserving bandwidth for emergency data is not efficient in terms of resource usage. At the same time, emergency data should be delivered on time without delay. To solve this problem, our proposed scheme differentiates the periodic data, and if the differences in the periodic data exceed a threshold, patient's personal wireless hub (PWH) reserves bandwidth on the wireless networks in order to ensure the availability of wireless bandwidth for the emergency data. This scheme reduces the wastage of bandwidth resources by not reserving bandwidth for emergency data all the time. At the same time, by predicting the occurrence of an emergency situation and reserving resources beforehand based on the prediction, it improves the probability of bandwidth availability under emergency situations.

In this paper, we consider the scenario of a mobile telemedicine device that has multiple wireless interfaces and that is capable of supporting multiple telemedicine applications. The mobile patient with a portable telemedicine device, called PWH in this paper, is considered to be in a low mobility, densely populated area such as a shopping mall as shown in Figure 1. The vital sign data of a mobile patient are transmitted in wireless medium from the patient's body sensors to PWH, where the body sensors form a body sensor network (BSN). In addition to body sensors, PWH is also capable of communicating simultaneously with other networks such as wireless sensor network (WSN), cellular network, and WLAN. Note that WSN provides context-aware data (e.g., temperature, location, and humidity level) to the patient's PWH, which helps interpret accurately the patient medical data. This paper addresses some security and/or channel allocation/reservation aspects of data transmission from body sensors to PWH (over BSN) as well as from PWH to hospital data centers (over wireless networks).

The sensors implanted on the human body to monitor parts of the body are called biosensors. These biosensors form a network and collectively monitor the health condition of their carrier or host. Health monitoring involves collection of data about vital body parameters known as biometric signals or biometric data, from different parts of the body and making decisions based on them [2]. As seen from Figure 1, remote patient monitoring uses body sensors to sense vital sign data for performing real-time health monitoring of patients. Because the system involves transmission of sensitive medical data, it should provide basic level of security. Key distribution is central to any security mechanism based on cryptographic techniques. Symmetric key cryptography requires establishment of a secret session key between the communicating parties. Since biosensors are placed on the human body, we can use them to derive the required inputs for security mechanism from the body. The establishment of this session key should be designed to conserve the limited energy resources of the body sensor. In this paper, we proposes an energy efficient secure key establishment and authentication (SKEA) protocol to establish a symmetric key between the body sensors and PWH using the biometric signals (e.g., heart rate interval, blood flow) of patients. This eliminates the use of expensive key generating functions and, therefore, the computational overhead is reduced.

Owing to its super-short communication range, the main security challenges faced by BSN include the following: (i) eavesdropping of data by a third party, unknown to the source as well as the receiver and (ii) modification and injection of data by third party without knowledge of the source and the destination. As sensors of BSN are expected to be interconnected on or in the human body, the body itself can form an inherently secure communication pathway that is unavailable to all other kinds of wireless networks. Biometrics recognition is based on "*who you are*" as opposed to/in conjunction with "*what you know*" *(PIN)* or "*what you have*" *(ID card)*. The problem of eavesdropping and the problem of interference between BSNs of different individuals boil down to one simple question: how can sensors or nodes of a BSN know that they belong to the same individual? The answer to this question lies in person's physiological or behavioral characteristics which can be used for identification and verification [3] purposes. It is desirable that all the nodes in a BSN share the same session key to communicate with PWH. Using traditional cryptographic techniques, it would be required to generate the session key at one node and then transmit it to all other nodes. However, it is always preferred not to transmit the actual key to be used over the network, even if it is encrypted using some other key. In such a scenario, since body sensors are placed on the same body, it becomes an attractive proposition to derive the required inputs for security mechanism from the body itself and to use the available biometrics for forming the session key without transmission of the actual session key over the network.

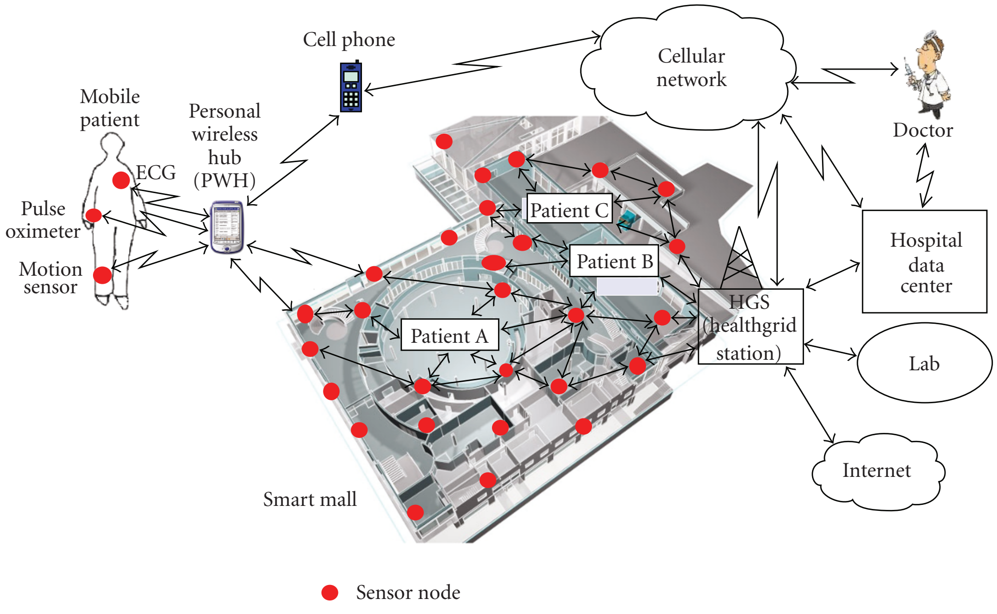

Figure 1: A mobile patient can communicate with hospital data center and/or physician through wireless networks (e.g., cellular and sensor networks), health grid station (HGS), and personal devices such as PWH.

A major concern with using biometrics for cryptographic purposes is the degree of randomness. Unless the biometric is random enough, an attacker can guess and compromise it, leading the false acceptance rate to be increased, where the false acceptance rate refers to the probability that the biometric security system allows an access attempt by an intruder. The level of randomness of any quantity is defined by the level of entropy [4]. The entropy can further be increased using a combination of readings at more than one instance of time because the search space is further increased. Some candidate biometrics and their ranges are shown in Table 2 [2, 5]. The ranges are mentioned for normal as well as abnormal conditions.

The contributions of this paper include the following: (i) a channel allocation and reservation algorithm that reserves bandwidth for emergency telemedicine data by measuring the vital signs and predicting the status of the patient, (ii) an adaptive priority and security assignment scheme to meet the delay of emergency medical data, (iii) a dynamic packet scheduling scheme that schedules packets on multiple interfaces based on the instantaneous QoS requirements of packets and channel conditions, and (iv) security algorithms for key establishment, confidentiality, and authentication between body sensors and PWH. The proposed channel and reservation algorithm differs from existing work in that it adapts the amount of resources reserved for emergency data based on the variations in patient's health conditions. In the proposed adaptive priority and security assignment scheme, when a patient is in critical situation, the strength of security is increased in data transmission from the PWH to the healthcare center if the patient is in good condition. A set of modules such as the classifier, scheduler, and channel allocator are used together to schedule packets of various applications through multiple interfaces and channels of different wireless networks.

The rest of the paper is organized as follows. Section 2 presents the related work. Section 3 presents the system model used in the paper. The proposed framework for adaptive secure channel allocation is presented in Section 4. The call admission control algorithm that reduces the call dropping probability of medical calls is presented in Section 5. Section 6 presents the secure data transmission algorithm over body sensor networks. The performance analysis is presented in Section 7. Concluding remarks are made in Section 8.

2. RELATED WORK

Third generation (3G) and beyond cellular networks provide support for multimedia data transmission [6]. For instance, 3G networks support a data rate of up to 144 kbps for vehicular users and a data rate of up to 2 Mbps for pedestrian users. In addition to providing higher data rates, 3G networks also have the advantage of providing continuous coverage in both urban and rural areas. Therefore, they are well suited for telemedicine applications that require continuous connectivity (periodic data). However, one disadvantage of 3G networks is that in hot spot areas such as airports, shopping malls, they may not have enough capacity to support all users because of heavy loads. Therefore, allocating some channels from alternative networks in hot spot areas would be required.

WLANs provide a cheap and effective alternative to cellular networks in hot spot areas [7]. With the emergence of technologies such as voice over WLAN, it is possible to maintain a voice call over a WLAN interface.

Table 2: Candidate biometrics with their ranges.

Biometric	Range
Blood glucose	64–140 mg/dL (varies with activity)
Blood pressure	120–160 mmHg (systolic) (range is from hypotension to hypertension)
Temperature	97.0–105.0 F (range across ages and normal and abnormal conditions)
Hemoglobin	12.1–17.2 g/dL (varies between male and female and age and altitude)
Blood flow	Greater than 0.9 ABI (normal) Less than 0.5 ABI (abnormal)

Further, WLANs provide higher data rates of up to 54 Mbps (802.11g). However, WLANs have very limited coverage. IEEE 802.16/WiMAX technology provides broadband connectivity in a wireless metropolitan area network (WMAN) environment for to both fixed and mobile users [8]. To provide flexibility for different applications, the standard supports two major deployment scenarios. In the last-mile scenario, broadband wireless connectivity is provided to home and business users in a WMAN environment. The operation is based on a point-to-multipoint single-hop transmission between a single base station (BS) and multiple subscriber stations (SSs). Backhaul networks is a multihop (or mesh) scenario where a WiMAX network works as a backhaul for cellular networks to transport data/voice traffic from the cellular edge to the core network (Internet) through meshing among IEEE 802.16/WiMAX base stations.

A notion for QoS for telemedicine multimedia data is presented in [9]. The authors elaborate on several synchronization protocols to achieve key multimedia telemedicine data synchronization requirements. In [10, 11], the telecommunication and QoS requirements of various telemedicine applications are presented. They also discuss how various technologies can be chosen to support the QoS requirements of telemedicine applications. But, they do not address how the various technologies can be integrated to support the QoS requirements of telemedicine applications. Integration of the networks is essential to support high bandwidth telemedicine applications. In [12], the transmission of visual sensor data is adapted based on the changes in patient's state.

Bandwidth allocation for telemedicine applications and bandwidth aggregation is addressed in [1, 13, 14] to ensure their QoS guarantees. However, these schemes do not consider bandwidth aggregation over multiple wireless networks. In [15–21], the authors propose to take advantage of bandwidth aggregation to meet the QoS requirements of bandwidth intensive telemedicine applications when the bandwidth of a single network is not sufficient to meet all the QoS requirements. In [15], a packet scheduling scheme where latency sensitive packets are sent over low latency timeslots is presented. Also, in [17], only a random way to find a schedule that maximizes the system utility is suggested. Another scheduling algorithm, called Earliest Delivery Path First (EDPF) in [18], schedules each path on the earliest delivery path, with the objective of reducing delay due to reordering and hence the delay and jitter experienced by the applications. The combination of Weighted Fair Queueing (WFQ) with EDPF is presented in [19] to ensure a fair share of the bandwidth among different applications. However, they do not address the multiple class traffic scenario. In [22], the authors propose a scheme to adapt the quality and security of transmitted video based on the channel status and patient status. Basically, a higher level encryption is used when the patient's status is urgent as compared to that used when the patient's status is normal. On the other hand, a higher level compression scheme is used when the channel quality gets poorer. These approaches ensure that the delay and the video quality of the telemedicine data are met in all circumstances. However, in our paper, we do not modify the security of the patient's data even when the patient is in urgent situation, since reducing the encryption strength can affect the reliability of the patient's data.

In [20], the authors propose a QoS-Aware Wireless Bandwidth Aggregation (QAWBA) scheme where mobile nodes use multiple independent paths through other mobile nodes to receive data from the base station. QAWBA integrates on-demand proxy discovery, bandwidth reservation and maintenance, and hop-by-hop routing to achieve this. The solution proposed is specific to 802.11 networks and does not consider heterogeneous networks. In [21], the presented scheme does not consider traffic of different traffic classes.

The ultimate aim of BSN is to provide a truly personalized monitoring platform that is pervasive, intelligent, context-aware, and invisible to the patient, thereby avoiding activity restriction or behavior modification. It should be noted that it is required by law that individual biometric data are kept in privacy [23]. Most of the research in the area of security for sensor networks is involved with generic sensor networks [24], which is not applicable to body sensor networks due to the fact that body sensors operate with extremely stringent constraints. For medical care, a sensor network platform is presented in [25], and the need for security in medical environment is addressed by considering ECC [26]. But all the security requirements are not adequately presented. Their ECC implementation over binary field $F_{2^{163}}$ (i.e., key length of 163 bits) takes about 34.2 seconds to compute a public-private key pair and another 32.4 seconds to compute a shared key via ECDH [26].

Bao [27] discusses the use of biochannel to assist secure transmission of privacy data. They assume an auto-shared secret (ASS) which is generated network-wide. They use the initialization key and the session key to complete a three-step security model. Researchers recently developed random-key predistribution protocols [28] which initially have a large pool of symmetric keys, and a random subset of the pool is distributed to each sensor node. In this, there is no need for a central authority but if an attacker compromises sufficiently many nodes, he could reconstruct the complete pool of keys and break the scheme. The proposed SKEA scheme uses no such pool and hence protects against such kind of attacks. Undercoffer et al. [29] present a scheme similar to [30] with the addition of addressing multihop communications. They use different keys to encrypt different parts of the packet like header and payload to ensure end-to-end security. Using different keys would incur overhead in terms of storage and computation which is not the case in the scheme proposed in this paper. Gupta et al. [31] create a web server implementing an ECC version of SSL running on server motes. The results indicate that it takes less than 4 s to complete an entire SSL handshake. However, this scheme uses ECDH to derive a shared key, which requires both the client and the server to have public keys. The work presented here does not assume the same.

With the growth of personal area networking (WPAN) technologies, the interest in healthcare monitoring, smart homes, and similar applications has grown significantly. ZigBee [32, 33] is the first industrial standard WPAN technology that provides short range, low power, and low data rate communication, and supports mesh networking and multihopping. Most of the existing systems lack two key features: (i) reliable wireless operation that conforms to standards, and (2) compatibility with smart home systems [34]. Established standards for wireless applications, such as Bluetooth and IEEE 802.11, allow high-transmission rates, but at the expense of high power consumption, application complexity, and cost. ZigBee networks, on the other hand, are primarily intended for low duty-cycle sensors, those active for less than 1% of the time. ZigBee is best described by referring to the 7-layer OSI model for layered communication systems. ZigBee gives the freedom to the developers to build custom applications which use the services provided by the lower layers of the 7-layer structure. It should be noted that the ZigBee uses an already existing data link and physical layers specification such as IEEE 802.15.4 standards for low-rate personal area networks.

3. SYSTEM MODEL

We assume that a number of body sensors forming a BSN are attached to a patient. Each patient is equipped with a portable device called PWH that is capable of gathering vital signs and context-aware data, processing and aggregating them, and transmitting them through its multiple wireless interfaces. PWH receives the context-aware data from nonmedical body sensors and wireless stationary sensors deployed in the area where patients roam. PWH is able to transmit and receive data to/from hospital data center via various wireless networks. PWH receives feedback from the wireless interfaces about the channel conditions. Based on the priority of the applications and the channel conditions, PWH schedules data packets on the appropriate interface so that the QoS requirements are met. Hence, PWH performs many operations including data aggregation, priority assignment, packet scheduling, and rate control.

Within PWH, data packets are transmitted from multiple application streams onto multiple wireless interfaces. We assume that an application flow F consists of a set of m subflows f_i, denoted by $F = f_1 < f_2 < \cdots < f_m$, for $1 \leq i \leq m$. The subflow f_i is transmitted only if those subflows whose indices are smaller than i are transmitted. The subflow f_1 provides the lowest quality for the application and each additional subflow improves the quality of the application. The rate requirements of the application can therefore be specified as $R = r_1 < r_1 + r_2 < \cdots < r_1 + r_2 + \cdots + r_m$, where r_i is the data rate requirement for subflow i. When the network bandwidth is available, we provide the rate requirement $r_1 + r_2 + \cdots + r_m$. When the network bandwidth is not available, we relax the rate requirement of the application. As for security model, we consider a multilevel security model similar to the one in [35]. Each security level corresponds to a different encryption and authentication scheme.

Though it is desirable to meet both the minimum delay and maximum rate requirements at the same time, it is not always possible to do so because of network load and channel dynamics. Whenever the minimum delay cannot be met for some subflows, the higher-order subflow need not be transferred. This reduces the delay, but at the same time reduces the quality of the application transmitted. Thus reducing the rate reduces the delay and vice versa. Similarly, reducing the security level reduces the delay encountered by a packet. In this paper, we adapt the security level used for transmission to meet the delay requirement of application in situations where QoS is more important than quality of protection (QoP).

We also assume that a patient exists in one of three states at a given moment with respect to a particular vital sign. At any given time, a patient's health status sign would be *good*, *fair*, or *critical*. A patient's health status is treated as *good* if the vital signs are stable and within normal limits. A patient's health status treated as *fair* if the vital signs show slight instability and the patient may be uncomfortable. For a patient whose vital sign data are unstable and not within normal limits, the patient's status is treated as *critical*.

4. PROPOSED FRAMEWORK

In this paper, we present our proposed framework that enables the transmission of telemedicine data over multiple wireless interfaces on a PWH. Figure 2 shows the various components of the PWH that enable the PWH to transmit the telemedicine data which are compromised of audio, video, images, and vital sign data. The basic idea behind the proposed framework is as follows. The *data differentiator* module performs the determination of status. The patient has different rate, delay, and security requirements based on his status. As a result, the bandwidth and security requirements of the vital sign data flows should be varied depending on the status of the patient. The proposed framework performs bandwidth and security adaption to meet the QoS and QoP of the telemedicine applications. The proposed framework treats the status of each vital sign distinctly, that is, a patient's status can be FAIR with respect to heartbeat reading, whereas it can be GOOD with respect to blood pressure at the same time. This allows the *classifier* module of the framework to give higher priority (static priority) to CRITICAL and FAIR flows over GOOD flows and thus provide better QoS to more urgent flows.

Although the assignment of a static priority based on the status of a flow allows the transmission of more urgent flows first, different flows of the same status can achieve different delays when they are transmitted on different wireless channels. Therefore, it becomes essential to prioritize further among flows of the same status based on their delay performance. To achieve this, the *scheduler* module assigns a dynamic priority to each flow based on its delay performance. The dynamic priority of all flows is set to 0 at their initiation. If the number of delay violations of a flow f_i exceeds the threshold $\mathrm{DT1}_i$, then the flow's dynamic priority is incremented by 1. Simply increasing the dynamic priority of a given flow in an unbounded manner will affect the performance of other flows with the same status. To address this issue, we reduce the strength of the security, thereby reducing the delays caused by the security schemes that are part of the end-to-end delay of a packet. Therefore, if the number of delay violations of flow f_i exceeds the threshold $\mathrm{DT2}_i$, then the security level of a flow is reduced by 1 as long as such a reduction is possible.

The total priority of a flow is determined by summing up both the static priority and dynamic priority. The flows are then sorted in nondecreasing order of their total priority. Since the PWH can transmit the data on multiple wireless interfaces over multiple wireless networks, the wireless channel with the lowest end-to-end delay among the available set of channels is determined. The head-of-line packet of a flow with highest priority is sent on the channel with the lowest end-to-end delay. The *channel allocator module* receives the delay feedback of each packet from the network and provides that information to the *delay monitor* module. The *delay monitor* computes the average delay, which is used by the *scheduler* module in determining the dynamic priority of packets of a flow.

The overall operation of the algorithm that executes on the PWH is shown in Algorithm 1. The algorithm takes as its input the data from various sensors, audio and video sources. Reference values REF_i that represent the value used as reference for vital sign i are also given as input. A set of thresholds VT_i and NCT_i for each vital sign i is also given as an input to the algorithm. These thresholds are used to monitor the changes in patient's health conditions with respect to a particular vital sign. The value of these thresholds is usually set by a doctor at the healthcare center. A pairwise key exists between the PWH and the healthcare center. Since the algorithm that runs on the PWH adapts the security levels to meet delay and other QoS requirements, the security algorithm is used and the strength of the encryption key is exchanged between the PWH and the healthcare center using this pairwise key.

The algorithm uses two counters $e\mathrm{count}_i$ and $n\mathrm{count}_i$. Counter $e\mathrm{count}_i$ counts the number of times that vital sign value i exceeds the reference value, whereas $n\mathrm{count}_i$ counts the number of times that vital sign value i does not exceed the reference value. The counters are all initialized to 0 on Lines 1 and 2. Lines 5 to 26 update the status of a patient's vital sign based on the values of $e\mathrm{count}_i$ and $n\mathrm{count}_i$. The current value of vital sign is obtained on Line 6. On Lines 7 and 8, the value of $e\mathrm{count}_i$ is incremented if the current value of vital sign is greater than the reference value. Otherwise, the value of $n\mathrm{count}_i$ is incremented on Lines 9 and 10. The status of the patient's vital sign i is changed to CRITICAL when the value of $[e\mathrm{count}_i/(e\mathrm{count}_i + n\mathrm{count}_i)]$ exceeds the threshold VT_i. Lines 13 to 16 handle the case when the patient's status with respect to vital sign i changes to CRITICAL. On Line 16, the PWH sends instructions to the body sensor network to update the period of measurement and security for vital sign i. Lines 18 to 20 handle the case when the patient's status with respect to vital sign i changes to FAIR. In this case, the patient still does not have CRITICAL data to transmit, but predicts the amount of additional bandwidth that would be required in case the patient enters into the CRITICAL state. This is done on Line 20. Lines 22 and 23 handle the case when the patient's state is GOOD. In this case, any additional bandwidth that was reserved in the FAIR state or used in the CRITICAL state is made free. Procedure SCHEDULE() is then called to schedule the packets on wireless channels.

The motivation behind reserving the additional bandwidth only in case of a patient's state becoming FAIR or CRITICAL is as follows. Under most circumstances, the PWH needs to send regular measurements from the body and send it to the healthcare center. The bandwidth required for this data is predictable and therefore it can be reserved ahead on these networks without incurring any resource wastage. Under CRITICAL situations, the PWH needs to send more measurements and even detailed images audio and video to the healthcare center. These applications require higher bandwidth and since they occur in such a sporadic fashion, reserving the resources for them all the time would cause huge wastage of resources. On the other hand, not reserving any bandwidth will decrease the probability of obtaining the additional bandwidth by a patient in a CRITICAL situation. Therefore, in order to provide a tradeoff between the above two cases, we start reserving the bandwidth when the patient's state becomes FAIR with respect to to a vital sign. The amount of reservation can be modified based on the predicted amount of bandwidth required and the probability of moving from the FAIR state to the CRITICAL state. This reduces the resource wastage and also increases the chances of obtaining bandwidth when the patient is in CRITICAL state. In Section 5, we present an algorithm that reduces the probability of call blocking when medical calls request additional bandwidth.

Procedure CLASSIFY is shown in Algorithm 2. The procedure checks if the flow has already been classified on Line 1. If the flow is not classified, it is assigned a security level on Lines 2 to 8. PRIO_1, PRIO_2, PRIO_3 are integers such that $\mathrm{PRIO}_1 < \mathrm{PRIO}_2 < \mathrm{PRIO}_3$, and s_1, s_2, s_3 are security levels such that $s_1 < s_2 < s_3$. The security level assigned to a flow is higher when the flow is in GOOD state. In CRITICAL situation, security level is reduced to meet other important QoS requirements such as delay. On Lines 11 to 16, the procedure assigns a static priority to each vital sign data flow. The vital

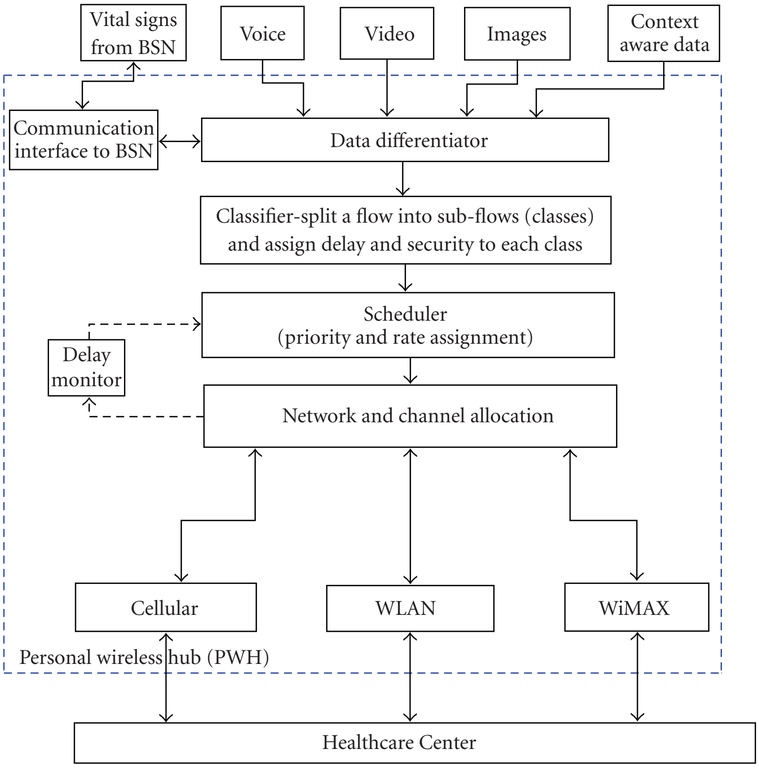
Vital signs from BSN
Voice
Video
Images
Context aware data
Communication interface to BSN
Data differentiator
Classifier-split a flow into sub-flows (classes) and assign delay and security to each class
Scheduler (priority and rate assignment)
Delay monitor
Network and channel allocation
Cellular
WLAN
WiMAX
Personal wireless hub (PWH)
Healthcare Center

Figure 2: Modules that constitute a PWH. Operation of the PWH.

sign data i that is CRITICAL state is assigned a higher value of static priority sp_i.

Procedure SCHEDULE shown in Algorithm 3 assigns a dynamic priority to the packet flows based on the delay violations and computes the total priority. The dynamic priority is initially set to zero and is incremented if the delay violations exceed threshold DV1_i on Lines 1 and 2. If the delay violations exceed threshold DV2_i, the security level of the flow is reduced to better meet the delay requirements. In this case, the dynamic priority is reset to zero. This procedure also determines the channel that is allocated to each packet. On Line 13, packet p with the maximum priority ap_i is determined. On Line 14, the channel c with lowest delay is determined. The packet p is sent on channel c on Line 15. The delay feedback is obtained and sent to the delay monitor. The delay feedback is used in determining the dynamic priority.

5. CALL ADMISSION CONTROL

We now present the dynamic channel allocation algorithm that is invoked whenever bandwidth is not available to satisfy a medical data call request for emergency data in a cellular network. The dynamic channel allocation algorithm presented here dynamically requests and migrates bandwidth from neighboring base stations. The base stations are responsible for bandwidth allocation. The load on all base stations is not going to be uniform. Also, every possible attempt should be made in order not to drop a medical data call. Therefore, a dynamic and adaptive channel allocation scheme is essential, where channels are shared dynamically by various base stations of the same network access technology by adapting to the requirements of the clients.

We present the following scenario that would require the transmission of medical video/images. Consider a patient who is under NORMAL circumstances. Only vital sign data such as ECG data are transmitted from the patient to the healthcare center. However, when the patient is in a CRITICAL state, he will probably be taken to the hospital in an ambulance. In this situation, high bandwidth data such as diagnostic medical images and videos need to be transmitted from the patient to the healthcare center. These data can be acquired either on an ambulance or by the patient himself using a camera. However, the focus of this paper is not about data acquisition. The transmission of these high bandwidth data without violating their QoS requirements requires the reservation of additional bandwidth.

The adaptive channel allocation algorithm presented in the paper achieves this by reserving additional bandwidth whenever it detects a change in the patient's state from GOOD to FAIR. The bandwidth is reserved for all medical data calls, and any medical data call can make use of this bandwidth reservation. This reservation is also done not just in the current cell, but also in the neighboring cells. This reduces the call blocking and call dropping probabilities

```
Input: A PWH with multiple network interfaces receives medical data from body sensors of the patient and other sources
       such as video and audio. A set of $\mathrm{REF}_i$ values that denote the reference values for each vital sign $i$. A set of thresholds
       $\mathrm{VT}_i$ and $\mathrm{NCT}_i$ for each vital sign $i$. Threshold $\mathrm{VT}_i$ represents the minimum number of times that vital sign value $i$
       has to exceed the reference value $\mathrm{REF}_i$ for that vital sign status to be changed to CRITICAL. Threshold
       $\mathrm{NCT}_i$ represents the minimum number of times that vital sign value $i$ has to be below the reference value $\mathrm{REF}_i$ for
       that vital sign status to be changed to GOOD from CRITICAL. Pairwise key between PWH and healthcare center.
Output: Medical data packets are assigned channels on appropriate network interfaces based on the channel conditions,
        QoS requirements, and urgency of the medical data packet.
begin
$e\mathrm{count}_i \leftarrow 0$ for all $i$.
$n\mathrm{count}_i \leftarrow 0$ for all $i$.
$P \leftarrow P_{\mathrm{INIT}}$, where $P_{\mathrm{INIT}}$ is the initial periodicity of measurement for vital sign data from the body sensors.
for every period do
    for every vital sign $i$ do
        $\mathrm{curr}_i \leftarrow$ current value of vital sign data $i$.
        if $(\mathrm{curr}_i > \mathrm{REF}_i)$ then
            $e\mathrm{count}_i + +$.
        else
            $n\mathrm{count}_i + +$.
        end if
        if $(e\mathrm{count}_i/(e\mathrm{count}_i + n\mathrm{count}_i) > \mathrm{VT}_i)$ then
            $\mathrm{status}_i \leftarrow$ CRITICAL.
            Get data from external sources.
            Call CLASSIFY($i$, CRITICAL).
            Decrease period $P$.
        else if $(\mathrm{curr}_i > \mathrm{REF}_i)$ AND $(e\mathrm{count}_i/(e\mathrm{count}_i + n\mathrm{count}_i) \leq \mathrm{VT}_i)$ then
            $\mathrm{status}_i \leftarrow$ FAIR.
            Call CLASSIFY ($i$, FAIR).
            Make additional bandwidth reservation $r_i$.
        else
            $\mathrm{status}_i \leftarrow$ GOOD.
            Call CLASSIFY ($i$, GOOD).
            Free additional bandwidth reservation.
        end if
    end for
    Call SCHEDULE().
end for
end
```

Algorithm 1: Algorithm PWH.

of high bandwidth telemedicine applications. The reduction in call blocking and dropping probabilities ensures that telemedicine applications do not experience any variation in QoS achieved.

The adaptive dynamic channel allocation (ADCA) algorithm presented in this section does the channel allocation to a medical or a nonmedical call. A base station uses a different frequency, time slot, or code for each connection with a client. We also assume that each BS knows its neighboring BSs, that is, the network is already established and it remains fixed. The base stations do not move, however the wireless clients can move from the coverage area of one base station to another. The ADCA scheme proposed supports both medical and nonmedical traffic. It is possible that some of base stations may become more loaded than the others. In such a situation, some channels have to be transferred from one base station to another.

The basic steps of the adaptive dynamic channel allocation (ADCA) algorithm are presented next. On Line 2, each base station computes and sends its call blocking probability for medical and nonmedical calls to all of its neighbors. Based on the knowledge of its own call blocking probabilities and of that of its neighbors, on Line 3, each base station determines whether a request can be made to borrow channels from any of the neighboring nodes. Based on the determination, neighboring channels are requested. If this base station receives a channel borrowing request from the neighboring node, it first checks if the number of free channels under the base station is greater than the threshold of free channels. If so, an appropriate free channel is moved from the base station to the requesting neighbor on Line 5. On Lines 6 to 9, a channel is allocated to a medical call. A medical call is assigned a channel as long as there are free channels available. On Lines 10 to 13, a channel is allocated to a nonmedical call.

```
Input: Flow id $f_i$ of the vital sign data $i$ and status$_i$ of the patient w.r.t vital sign $i$. CLASSIFIED$_i$ is FALSE for all flows
        initially. PRIO$_1$, PRIO$_2$, PRIO$_3$ are integers such that PRIO$_1$ < PRIO$_2$ < PRIO$_3$. $s_1$, $s_2$, $s_3$ are security levels such
        that $s_1 < s_2 < s_3$.
Output: Assigns a static priority sp$_i$ to flow $i$ based on the status$_i$ of the vital sign $i$ of the patient.
begin
   if (CLASSIFIED$_i$ == FALSE) then
      CLASSIFIED$_i$ ← TRUE
      if (status$_i$ == CRITICAL) then
         security$_i$ ← $s_1$.
      else if (status == FAIR) then
         security$_i$ ← $s_2$.
      else
         security$_i$ ← $s_3$.
      end if
   end if
   if (status$_i$ == CRITICAL) then
      sp$_i$ ← PRIO$_3$.
   else if (status == FAIR) then
      sp$_i$ ← PRIO$_2$.
   else
      sp$_i$ ← PRIO$_1$.
   end if
end
```

Algorithm 2: Procedure CLASSIFY.

```
Input: Static priorities sp$_i$ assigned by classifier and the delay feedback df$_i$ from the delay monitor. Two delay violation
        thresholds DV1$_i$ and DV2$_i$, such that DV1$_i$ < DV2$_i$. Dynamic priority of each flow dp$_i$ is initially set to zero.
Output: Computes aggregate priority ap$_i$ by adding a dynamic priority to the static priority of each packet.
begin
   if (df$_i$ > DV1$_i$ and (df$_i$ ≤ DV2$_i$)) then
      dp$_i$ + +.
   else if (df$_i$ > DV2$_i$) then
      if (security$_i$ > $s_1$) then
         security$_i$ − −;
         dp$_i$ ← 0.
      end if
   else
      if (dp$_i$ > 0) then
         dp$_i$ − −.
      end if
   end if
   ap$_i$ ← sp$_i$ + dp$_i$ for all $i$.
   while there are unscheduled packets and unassigned channels do
      Determine the packet $p$ with the maximum priority ap$_i$.
      Determine the channel $c$ with the lowest delay.
      Send packet $p$ on channel $c$.
      Determine one-way delay $p$th_delay for packet $p$ from the PWH to the healthcare center based on the feedback
        received from the healthcare center.
      Send $p$th_delay to the Delay Monitor; The Delay Monitor updates a database of average $p$th_delays as delay feedback
        df$_i$ for each vital sign data flow $f_i$.
   end while
end
```

Algorithm 3: Procedure SCHEDULE.

```
Input: A wireless network has $N$ channels and $M$ base stations. Initially, each BS is assigned an equal number of channels.
Output: Based on the blocking probabilities of medical and nonmedical calls, channels are dynamically assigned among BSs.
        Channels are allocated to reduce the blocking and dropping probabilities of medical calls.
begin
for each base station, $BS_i$ do
    base station $BS_i$ first computes the blocking probabilities of medical and nonmedical calls and sends
    this information along with the list of occupied channels to the neighboring base stations.
    Using the information of blocking probabilities in the local and the neighboring base stations, base station $BS_i$ decides
    whether a request should be made to move an appropriate free channel from neighboring base stations,
    and then implements its decision.
    if (number of free channels under base station, $BS_i$ > TFC) and (a neighboring base station requests a free channel)
    then
        An appropriate free channel is moved from base station $BS_i$ to the neighboring base station requesting a free channel.
    else if (a medical data call arrives) then
        if (a free channel is available) then
            Assign a free channel to the medical data call.
        end if
    else if (a nonmedical data call arrives) then
        if (number of free channels under base station $BS_i \geq$ TGC) then
            Assign a free channel to the new call.
        end if
    end if
end for
end
```

Algorithm 4: Algorithm ADCA.

A nonmedical call is allocated a channel only if the number of free channels is greater than the threshold of guard channels, TGC.

The ADCA algorithm makes use of two thresholds while assigning channels to a patient data or a nonpatient data call. This is similar to the scheme used in our earlier work [36] where the purpose of the two thresholds is to reduce the handoff call dropping probability. In this paper, the objective is to ensure low call blocking probability for patient data calls. Every base station maintains two thresholds, TFC and TGC, where TFC is the threshold of free channels and TGC is the threshold of guard channels for medical data calls (TFC > TGC). Every base station periodically sends the call blocking probabilities of patient and nonpatient calls to its neighbors. A nonmedical call is assigned a channel only when the number of free channels under the base station is greater than TGC, that is, TGC number of channels is always reserved for patient data calls. In situations when a patient data call cannot be allocated a channel even from the set of guard channels, the algorithm attempts to transfer a channel from a neighboring base station. A base station is allowed to transfer a channel only when the number of free channels under that base station is greater than TFC. Since TFC is greater than TGC, this transfer of channels does not affect the call blocking probability of patient data calls under the base station that transfers the channels.

6. SECURITY WITH BIOMETRICS IN BSN

This section presents the algorithm SKEA to securely establish symmetric keys between the body sensors of BSN and PWH. The main concern when dealing with security within sensor networks is to securely generate and distribute the session key for secure communication. In this regard, we first state our assumptions.

6.1. Assumptions

(1) At the point of deployment, the body sensors are embedded with a common global key, K_{CG}, and authenticated at a secure place. This key is assumed not to be compromised at the start. This key is initially used to set up the session key at a secure place and then deleted. New current common global key can be established using the *key chaining using reconciliation* phase proposed.

(2) The biometrics used to establish the session key provide good degree of randomness so that an attacker would not be able to guess it and compromise the security of the system.

(3) A body sensor is assumed not to be compromised when initially attached to the patients body.

(4) The matching of two biometric signals is based on the confidence value used. In this paper, we assume a confidence value of 90%.

(5) An intruder either eavesdrops or injects false data but cannot physically destroy the body sensor.

6.2. Source authentication

Whenever a sensor sends some information to the PWH, the source of the data needs to be authenticated to make sure that an intruder is not forging the data. We propose the use of physiological signals from the biometrics along with a voting mechanism to achieve the same. After establishment of a secure session key, we need to provide data confidentiality and data integrity for the transmitted data from the body sensors to the PWH. We can provide data confidentiality by encrypting the data with the session key established. To provide data integrity, we use HMACS with a key as an input. To make it more secure from intruders, the key used for data confidentiality should be different from the key used to establish data integrity (to calculate the HMAC). Using this scheme, an intruder will need to have the knowledge of both keys in order to spoof the PWH.

6.3. Using ECG signals

ECG sensors placed at different places on the body send their analog signals to the personal wireless hub (PWH) where they are combined and only one ECG signal is produced. Authors in [37] present the PQRST wave for an ECG signal under normal and abnormal circumstances. Also in [38], authors present a table with values of ECG signals under normal conditions and under hypertension. For a given patient under normal circumstances, an ECG signal exhibits the following characteristics [39].

(1) Normal characteristics of the P wave

  (a) smooth and rounded
  (b) no more than 2.5 mm in height
  (c) no more than 0.11 sec in duration
  (d) positive in leads I, II, aVF, and V_2 through V_6.

(2) Normal characteristics of the ORS complex

  (a) normal duration of the QRS complex in an adult varies between 0.06 and 0.10 second
  (b) a normal Q wave is less than 0.04 second in duration and less than 1/3 of the amplitude of the R wave in that lead.

(3) Normal characteristics of the T wave

  (a) slightly asymmetric
  (b) T waves are not normally more than 5 mm in height in any limb lead or 10 mm in any chest lead; T waves are not normally less than 0.5 mm in height in leads I and II.

At the time of deployment, the ECG signal of the patient is recorded under normal status and stored in the PWH. For every subsequent ECG signal generated at the PWH, it is compared with the stored ECG signal, and the decision regarding the status of the patient is made based on the comparison.

6.4. MAC and subMAC

Keyed-hash message authentication codes or HMACs are used to ensure authenticity of the data received. We propose to use keyed MACs which in addition to providing data authenticity also provide data integrity. The TinyOS data packet structure [40] includes 29-byte payload. In the proposed scheme, HMAC is calculated over the data to be transmitted and the calculated HMAC is transmitted along with the data. The calculated HMAC is 16 bytes long. Thus, using HMACs introduces communication overhead of 16 bytes for every message transmitted. This kind of overhead is not desirable in an already resource constraint body sensor. In order to reduce the same, we propose the use of subMAC. A subMAC is constructed by selecting some bits of an HMAC. With the use of subMAC, we reduce the overhead by transmitting only a part of the actual HMAC rather than the entire HMAC. For calculation of keyed-hash MAC, we assume the transmitter and the receiver have a shared common global secret key, K_{CG}.

To form a subMAC from an HMAC, certain bits are selected. To select these bits, we assume that each sensor node has the same pseudo random number generator (PRNG) [41]. This generator is used to generate random numbers between 1 and 32. The sensor nodes initiate their PRNG using their current global key as the seed. The sensor node S_i first computes the HMAC of the data using the current global key K_{CG} which is embedded into every sensor at the point of deployment. To select certain bits from the HMAC, S_i runs its PRNG eight times which results in eight random numbers between 1 to 32. Each random number indicates the index of a bit location in HMAC, and the bits of those selected locations constitute the subMAC. The transmitter then sends this subMAC to the intended receiver. To verify this subMAC, the receiver similarly computes HMAC of received message and runs its PRNG eight times with the current global key as the seed to generate the subMAC. If the subMACs match, the message is said to be authenticated by the receiver. There is a tradeoff with using subMACs. While transmitting less number of HMAC bits, we help reduce the transmission overhead but at the same time we also compromise the security level in terms of authentication strength. An intruder can more easily forge a 1 byte HMAC than a 16 byte HMAC. The desired level of security can be achieved by running the PRNG more number of times to select more of the HMAC bits to form the subMAC. Hence the size of the subMAC is directly related to the strength of the authentication process and the communication overhead. A balance needs to be achieved between the desired security level and the transmission overhead.

6.5. Key chaining using reconciliation

It is assumed in the proposed algorithm that there exists a common global key, K_{CG}, which is available at the start of the system. This key is used for secure communications between the body sensors and PWH while establishing the session key. Owing to security concerns, this common global key should be changed from time to time in order to avoid any intruder to compromise a node and get the value of the current common global key. This change is initiated by the PWH which prevents any compromised node to forcefully change the current common global key. We use the reconciliation scheme [42] in order to derive the new common global key. Thus, in order to establish a session key for every subsequent session, the sensor and PWH use the current common global key.

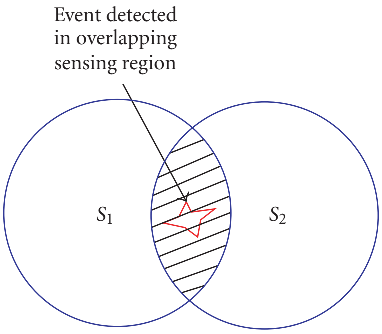

Figure 3: Overlapping sensing region for key reconciliation.

Consider the scenario shown in Figure 3. We have two sensors say S_1 and S_2 which detect the same event. These two sensors can communicate with each other and zero in a secret key based on the sensed event. In the proposed scheme, the PWH requests two sensor nodes for their sensed biometric signals. Sensors S_1 and S_2, having their sensing regions overlapping, send the sensed biometric signal to PWH. Upon receiving the signal, PWH compares them with its original signal and prepares the index where the signals match, that is, they have a confidence value greater than 90%. PWH encrypts these indices and sends them back to the sensors where decryption takes place. Sensors upon reading the indices send by the PWH, compute the new current common global key which is used from next session onwards.

6.6. Algorithm SKEA

At the start, two body sensors say S_1 and S_2 perform mutual authentication with PWH with the help of nonce(s) and subMACs. Now say if sensor S_3 wants to communicate with PWH, it establishes a symmetric session key K_S with PWH. Any body sensor requesting for a session key communicates with any other two body sensors which already have performed mutual authentication with the PWH. Here we assume that sensors S_1, S_2, and S_3 have overlapping sensing regions and can sense the same event or the same biometric signal. The steps for the same event are as follows and are given in Algorithm 5.

Step 1. Sensor S_1 sends its biometric reading H_1 to the personal wireless hub (PWH) along with the subMAC of the message.

Step 2. PWH on receiving the biometric reading calculates the subMAC of the message to establish integrity of the message. PWH then compares H_1 with its predefined value and stores the indices as I_1 where they match (calculation of confidence value). PWH then deletes this reference to make sure that if the value of the biometric changes, it does not use the old reference value. This reference value is changed dynamically using the most recent data transmission from the body sensor.

Step 3. Sensor S_2 sends its biometric reading H_2 to PWH along with the subMAC of the message.

Step 4. PWH on receiving H_2 calculates the subMAC of the message to establish message integrity. It then checks the values at indices I_1 and picks the indices where the values match (calculation of confidence value).

Step 5. PWH sends these indices to all body sensors, and the sensors pick up values at those indices which form the common session key. The selected keys are expanded in order to form a 64-bit long session key.

Step 6. Sensors use this session key to communicate with the PWH. Sensors also compute per sensor session key by combining the common session key with the pairwise key established during the initial authentication phase. In order to hide data from other sensors, a sensor can use its per sensor session key to communicate with the PWH.

Step 7. With the transmission of actual data, PWH keeps storing the actual biometric signal measurement as the reference for establishment of the next session key as this stored value will have a high correlation with the biometric reading used by the sensor to establish the next session key.

6.7. Secure data transmission

Once a session key is securely established between the body sensors and the PWH, the body sensors can use this session key for transmitting the data securely to the PWH. The established session key is known globally by all the body sensors and the PWH. Each body sensor also establishes a pairwise key with the PWH which is only known to the corresponding sensor and the PWH. Each body sensor provides data confidentiality by encrypting the data with the session key and uses the pairwise key for data authentication.

6.8. Security analysis

The use of confidence values helps prevent forging of the data. Using this value, PWH can make out if the message is send by a legitimate sensor or an intruder. The use of confidence values helps in reducing the crosstalk interference among body sensors of different subjects. The intermediate session key established is based on both the confidence values and hence in order to forge this value, the intruder has to compromise both nodes generating the confidence value.

Body sensors S_1, S_2, and S_3 form a three-party communication scheme. In the proposed protocol, sensors S_1 and S_2 authenticate S_3 using the biometric signal of S_3. While establishing the intermediate session key, S_1 and S_2 authenticate each other and finally S_3 authenticates S_2 using the original nonce. Only sensor S_1 is not authenticated by S_3.

Considering a situation where one of these two body sensors, either S_1 or S_2 gets compromised. If sensor S_2 gets compromised, when it send its confidence value to S_1, S_1 looking at its confidence value can establish if S_2 is compromised

```
Input: $S_{ID}$: ID of the body sensor which wants to communicate with PWH. Its length is 5 bits.
$H_{ID}$: Biometric signal sensed by sensor $S_{ID}$.
$S_1$ and $S_2$: Two sensors we assume to have already been authenticated by PWH.
$K_{CG}$: System-wide symmetric key embedded at the point of deployment which is deleted after initial session key is established.
    Its length is 64 bits.
$K_i$: Pairwise key between the body sensor and PWH established during initial authentication phase. Its length is 64 bits.
$V_{threshold}$: Threshold to calculate the confidence value.
Output: $K_S$: A session key of 64 bits is established between $S_{ID}$ and PWH.
begin
  (1) At body sensor $S_1$ generates a random number, $n_1$ to be used as a nonce for $S_1$ and measure the biometric trait say $H_1$.
  (2) Prepare the message as $[S_1, PWH_{ID}, E_{K_{CG}}(H_1 \oplus K_1, n_1), subMAC_{K_{CG}}(S_1, PWH_{ID}, n_1)]$ and send it to PWH.
  (3) At body sensor $S_2$ generates a random number, $n_2$ to be used as a nonce for $S_2$ and measure the biometric trait say $H_2$.
  (4) Prepare the message as $[S_2, PWH_{ID}, E_{K_{CG}}(H_2 \oplus K_2, n_2), subMAC_{K_{CG}}(S_2, PWH_{ID}, n_2)]$ and send it to PWH.
  (5) At PWH, decrypt the message from $S_1$ and $S_2$, calculate subMAC, and compare with the received subMACs from sensors
      $S_1$ and $S_2$. Compare the received biometric trait, $H_1$ and $H_2$ with the reference biometric, $H_{ref}$ to calculate the confidence
      value, $V_{Conf}$. By comparing the three biometric readings, prepare indices where the three match.
  (6) Prepare message $[PWH_{ID}, S_1, E_{K_{CG}}(\text{indices} \oplus K_1, n_1, PWH_{ID}), subMAC_{K_{CG}}(S_1, PWH_{ID}, n_1, n_{PWH})]$ and send to $S_1$.
  (7) Prepare message $[PWH_{ID}, S_2, E_{K_{CG}}(\text{indices} \oplus K_2, n_2, PWH_{ID}), subMAC_{K_{CG}}(S_2, PWH_{ID}, n_2, n_{PWH})]$ and send to $S_2$.
  (8) At $S_1$ receive the message form PWH, decrypt using $E_{K_1}$ and extract the indices, nonce $n_1$ and $n_{PWH}$. Calculate and
      compare received subMAC to establish data integrity.
  (9) At $S_1$ compare the received nonce with the one sensor $S_1$ send in its original message to protect against replay attacks.
  (10) if ((subMAC check ok) and (nonce matches)) then
  (11)     Calculate session key, $K_S$ by picking values at indices send by PWH from the biometric reading. Expand the session key
           to make it into a 64 bit session key.
  (12) end if
  (13) At $S_2$ receive the message form PWH, decrypt using $E_{K_2}$ and extract the indices, nonce $n_2$ and $n_{PWH}$. Calculate and
       compare subMAC to establish data integrity.
  (14) At $S_2$ compare the received nonce with the one sensor $S_2$ send in its original message to protect against replay attacks.
  (15) if ((subMAC check ok) and (nonce matches)) then
  (16)     Calculate session key, $K_S$ by picking values at indices send by PWH from the biometric reading. Expand the session key
           to make it into a 64-bit session key.
  (17) end if
  (18) At $S_1$, calculate the per sensor session key $K_{S_1} = K_S \oplus K_1$.
  (19) At $S_2$, calculate the per sensor session key $K_{S_2} = K_S \oplus K_2$.
end
```

Algorithm 5: SKEA: symmetric session key establishment.

or not, and if compromised S_1 can send a message to PWH stating the compromised state of S_2 and PWH can further broadcast the same eliminating the body sensor S_2 from any further communications.

In a case where sensor S_1 gets compromised, it will try to send a compromised intermediate session key to PWH. Since S_2 is not compromised, it will send the correct intermediate session key to S_3. Now, since both sensor S_3 and PWH will compute different session key, PWH upon receiving the message from legitimate sensor, S_3 will not be able to decrypt the message and hence we can conclude that it was given a wrong intermediate session key by sensor S_1 concluding that it has been compromised. PWH then can broadcast a message stating the compromised state of sensor S_1 so that it can be excluded from any further communications.

In case that both the sensors S_1 and S_2 are compromised, they can collaborate and send compromised intermediate session key to both sensor S_3 and the PWH. In such a case, the security of the proposed scheme can be broken, but it is highly unlikely that both the sensors chosen to form the intermediate session key are compromised as they previously have been authenticated by the PWH.

7. PERFORMANCE EVALUATION

7.1. Blocking probability

We first evaluate the blocking probability of medical and nonmedical data calls achieved by the proposed ADCA algorithm. To evaluate the blocking probability performance, a simulation environment consisting 20 serving nodes and 200 PWHs in an 1000 × 1000 meters area is used. The serving nodes and PWHs are distributed randomly. The coverage area of each serving node is fixed at 150 meters. Each wireless client associates itself to the nearest serving node. The traffic that is offered to the network has a uniform spatial distribution with Poisson arrival rates varying from 1 to 10 calls per second and an exponentially distributed call holding time of about 10 seconds. The data rate requirement of each call is varied uniformly between 75 bits per second to 600 bits per second. To evaluate the proposed algorithms, multiple simulation runs are performed.

The blocking probability of medical and nonmedical calls is used as the performance metrics. These two metrics are compared for different values of TFC and TGC. The objective of the performance evaluation is to identify the impact of TFC and TGC on the blocking probabilities at different loads and then to identify the best values of TFC and TGC at each load so that the blocking probability of medical calls is reduced significantly without affecting the blocking probability of nonmedical calls much.

The blocking probability is calculated as the ratio of dropped calls to the arrived calls in the entire network. The proposed algorithm works for any network. For example, the bandwidth resources that are transferred from one base station to another are timeslots in the case of a GSM network, whereas they are CDMA codes in the case of a WCDMA or CDMA-2000 network. Thus the algorithm is very generic and can be applied to any network that partitions bandwidth based on timeslots, codes, or frequencies.

Figure 4 shows blocking probabilities of nonmedical calls against offered traffic load for different values of TFC and TGC. For almost all of the values of TFC and TGC, the blocking probability remains low at very low loads of about 20 erlangs and it starts to increase significantly after that and stays almost constant and close to 1 after that. Call blocking probability is the highest when TFC and TGC are high and is low for lower values of TGC. Figure 5 shows blocking probabilities of medical calls against offered traffic load for different values of TFC and TGC. The value of call blocking probability for medical calls is minimum when TFC and TGC are large, that is, 0.9. This is because of reserving channels for medical calls, and allowing a higher value of TFC allows less channels to be borrowed from neighbors. Also it is evident from the figure that TGC affects the blocking probability of medical calls more than TFC. For the same value of TGC, a higher value of TFC results in lower call blocking probability. Figure 6 shows the traffic blocking probability against offered traffic load. The reason for showing the traffic blocking probability is because unlike conventional systems, the calls here have different rates and so blocking a call does not directly correspond to a proportional amount of traffic to be blocked.

7.2. Average delay and delay violations

Figure 7 shows the average delay experienced by the packets. The proposed scheme in this paper is labeled as PWH and is compared with earliest delay path first (EDF) algorithm. The EDF algorithm schedules the packet with the earliest deadline on the channel with the lowest delay. As can be seen from the figure, the proposed scheme achieves lower delay than the earliest-deadline-first policy. The adaptive security scheme allows the AHM scheme to achieve lower delay than the EDF scheme. Figure 8 shows the delay violations experienced by packets. The delay deadline is set to 500 milliseconds. Again, because of the reduction in the encryption delay, AHP achieves lower delay violations than the EDF scheme.

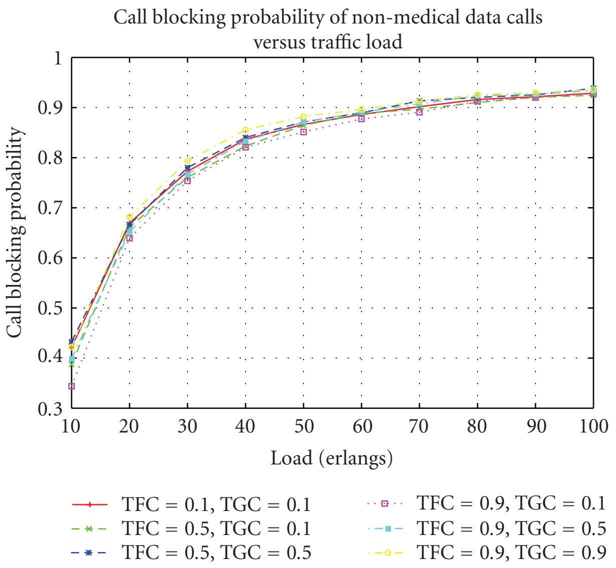

Figure 4: Call blocking probability of nonmedical calls versus traffic load.

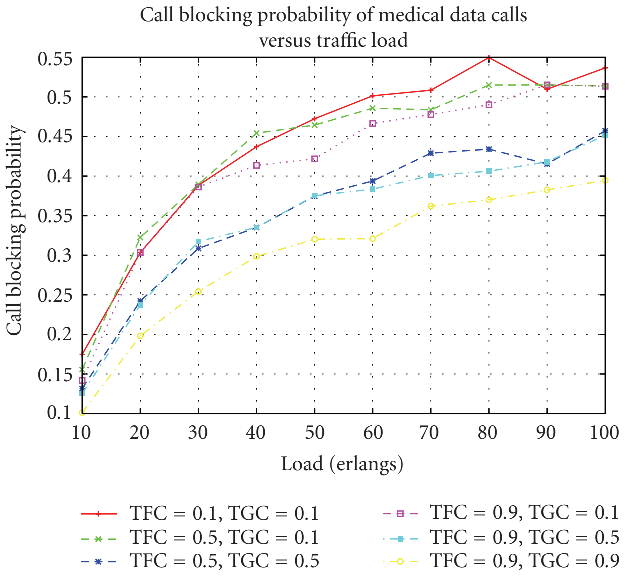

Figure 5: Call blocking probability of medical calls versus traffic load.

7.3. Communication overhead for algorithm SKEA

The SKEA algorithm is simulated using TinyOS [40] and PowerTOSSIM [43, 44]. The proposed SKEA algorithm uses keyed MACs for authentication purposes. In particular, we use MD5 [45] for calculating the keyed MAC with common global key, K_{CG}, which contributes to the communication overhead. Thus owing to the use of subMACs for each message, SKEA incurs an overhead of 1 byte. With the given payload size of 29 bytes, the communication overhead is reduced with the help of subMAC scheme from 16 bytes (without using subMACs) to 1 byte or from 55.17% to 3.45% of the

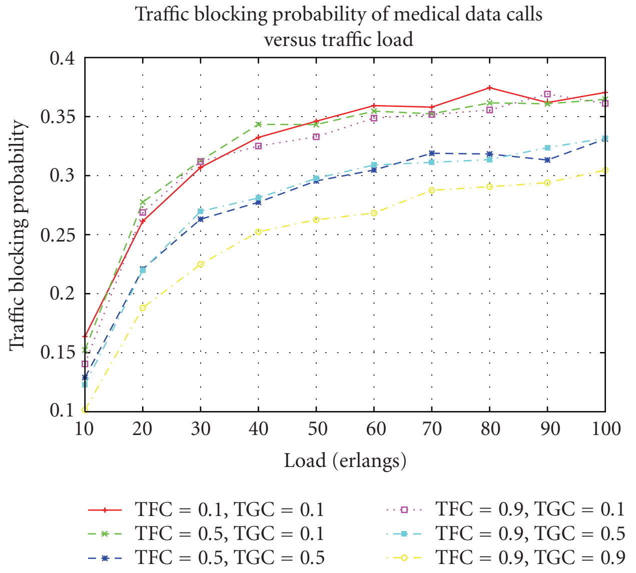

Figure 6: Traffic blocking probability of medical calls versus traffic load.

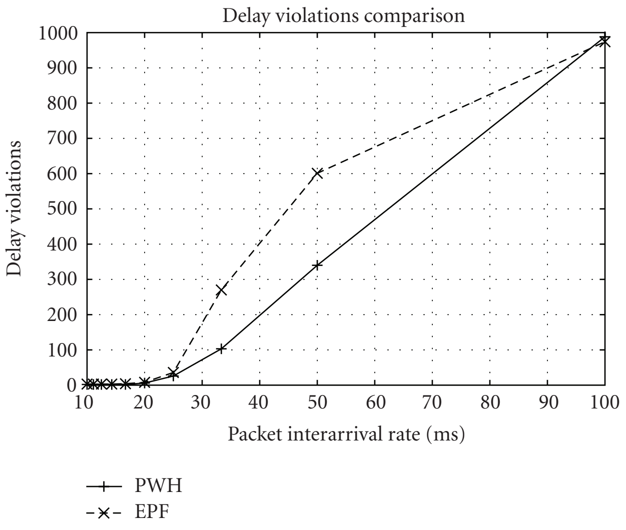

Figure 8: Delay violations versus load.

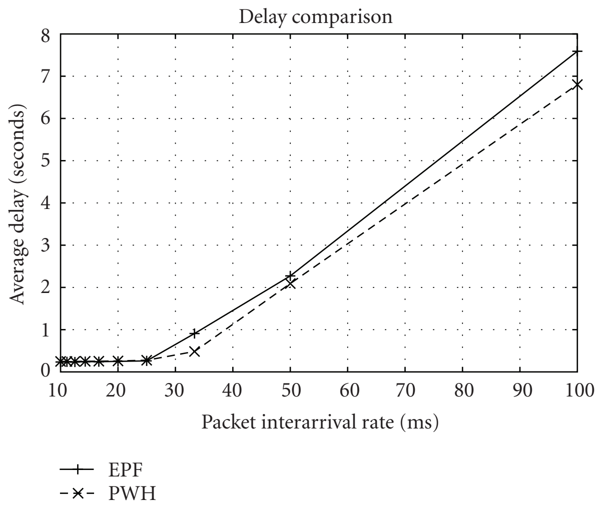

Figure 7: Average delay versus load.

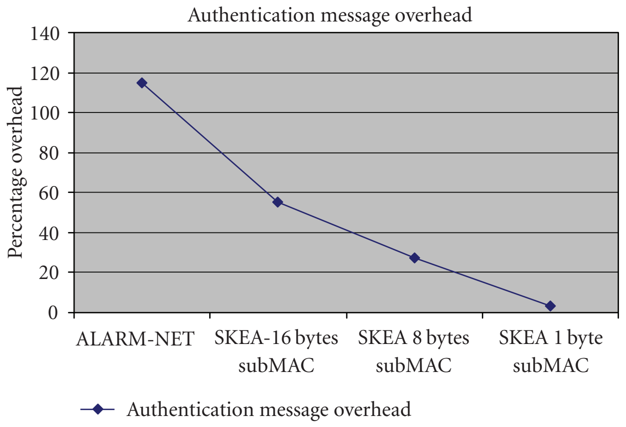

Figure 9: Message authentication percentage overhead (ALARM-NET versus SKEA).

payload size. With the use of keyed subMACs, we ensure data integrity and authenticity with minimal overhead.

Comparing with ALARM-NET, we see that for providing authentication only with a payload of 29 bytes, ALARM-NET reports to have a percentage overhead of 115% [46]; whereas using SKEA with subMAC of 1 byte we see an overhead of 3.45%. Figure 9 shows the percent overhead for ALARM-NET and SKEA with variable subMAC sizes of 16, 8, and 1 byte.

7.4. *Energy consumption for algorithm SKEA*

Since body sensors have stringent power constraints, any protocol designed for body sensors must use the available energy efficiently. Our aim is to provide desired level of security while utilizing the least amount of additional energy as overhead. Energy consumption is a very important performance metric for analysis of any security algorithm in wireless sensor networks. The SKEA algorithm is simulated using TinyOS [40] and PowerTOSSIM [43, 44].

We now analyze the energy consumption overhead of using HMAC authentication with SKEA protocol for the symmetric key establishment phase. We simulate two scenarios, first in which we perform key establishment using SKEA (with HMAC authentication) and the second key establishment using modified SKEA (without HMAC authentication). We analyze the overhead that is caused by using HMAC authentication in terms of energy consumption.

We calculate energy consumption in terms of CPU energy, radio energy, and total energy. The numbers for total energy required per body sensor for 5, 10, and 15 sensors are plotted in Figure 10.

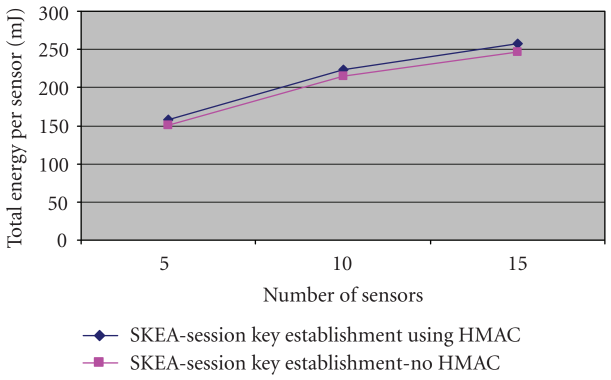

FIGURE 10: Total energy required per sensor to establish session key using SKEA (with and without HMAC authentication).

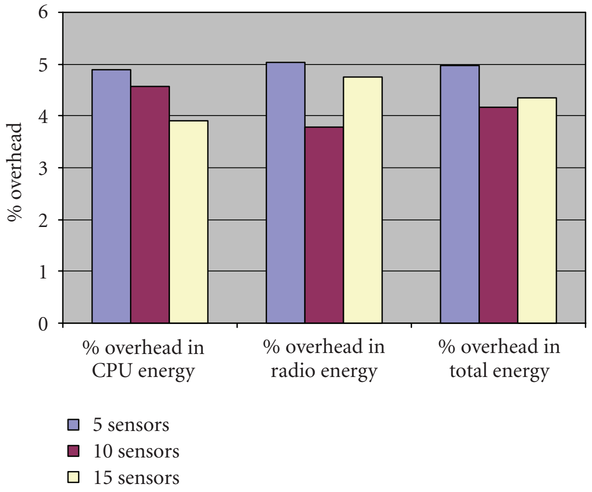

FIGURE 11: Percentage energy overhead using SKEA—Symmetric session key establishment (with and without HMAC authentication).

We observe that for all scenarios the total energy per sensor node for using HMAC authentication with SKEA is slightly higher (about 5%) than the case of not using HMAC authentication. Thus the proposed algorithm provides data integrity and authenticity using keyed MACs with a minimal overhead of about 5% in terms of energy consumption.

The percentage overhead in terms of radio energy, CPU energy, and total energy spent using the symmetric session key establishment scheme with HMAC authentication in SKEA is depicted in Figure 11. This figure shows that the SKEA scheme with HMAC authentication results in an energy overhead of 4%–5% in terms of CPU, radio, and total energy. But using keyed MAC, data integrity and authenticity are supported and, therefore, the small overhead is justifiable.

8. CONCLUSION

This paper has presented channel allocation algorithm and packet scheduling algorithms that collaborate with an adaptive security scheme. Since wireless channels exhibit highly varying channel conditions and have limited capabilities, mobile telemedicine applications in the proposed algorithms take advantage of all the available wireless networks to be able to meet their QoS requirements. The main feature of the proposed priority assignment technique is to update priorities dynamically and adapt security based on whether packets meet their delay over networks with different characteristics. Due to the importance of patient calls, base stations of wireless networks reserve some channels for patients calls depending on those thresholds that can cause minimal degradation in performance for nonpatient calls. The paper uses data differentiation to determine the status of the patient and predict the additional bandwidth that may be required by the patient in future. Using this scheme, the paper provides a higher channel availability for emergency medical data without reserving the network resources all the time.

This paper has also presented an energy efficient key establishment scheme SKEA for body sensor networks. SKEA uses biometric signals to generate a session key. The scheme uses keyed message authentication codes for authentication purposes. The use of biometrics to generate the session key eliminates the need of computationally expensive key generating functions. Moreover, biometrics reduces crosstalk interference between different subjects and avoids possibility of reflection attacks in a challenge-response protocol.

REFERENCES

[1] J. R. Gállego, A. Hernández-Solana, M. Canales, J. Lafuente, A. Valdovinos, and J. Fernández-Navajas, "Performance analysis of multiplexed medical data transmission for mobile emergency care over the UMTS channel," *IEEE Transactions on Information Technology in Biomedicine*, vol. 9, no. 1, pp. 13–22, 2005.

[2] S. Cherukuri, K. K. Venkatasubramaniam, and S. K. S. Gupta, "BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Procedings of the 32nd International Conference on Parallel Processing Workshops (ICPPW '03)*, p. 432, Kaohsiung, Taiwan, October 2003.

[3] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.

[4] November 1995, Cryptographic Random Numbers Standard P1363: Appendix E.

[5] US National Library of Medicine, "Mediline plus medical encyclopedia," http://www.nlm.nih.gov/medlineplus/encyclopedia.html.

[6] H. Holma and A. Toskala, *WCDMA for UMTS*, John Wiley & Sons, New York, NY, USA, 2002.

[7] S. Mangold, S. Choi, P. May, O. Klien, G. Hiertz, and L. Stibor, "IEEE 802.11 e wireless LAN for quality of service," in *Proceedings of the European Wireless*, vol. 18, pp. 32–39, Florence, Italy, February 2002.

[8] A. Ghosh, D. R. Wolter, J. G. Andrews, and R. Chen, "Broadband wireless access with WiMax/802.16: current performance benchmarks, and future potential," *IEEE Communications Magazine*, vol. 43, no. 2, pp. 129–136, 2005.

[9] A. Bhargava, M. F. Khan, and A. Ghafoor, "QoS management in multimedia networking for telemedicine applications," in

Proceedings of the 1st IEEE Workshop on Software Technologies for Future Embedded Systems (WSTFES '03), pp. 39–42, Hakodate, Hokkaido, Japan, May 2003.

[10] P. Nanda and R. C. Fernandes, "Quality of service in telemedicine," in *Proceedings of the 1st International Conference on the Digital Society (ICDS '07)*, p. 2, Guadeloupe, French Caribbean, January 2007.

[11] I. Reljin and B. Reljin, "Telecommunication requirements in telemedicine," *Annals of the Academy of Studenica*, vol. 4, pp. 53–61, 2004.

[12] W. Luh, D. Kundur, and T. Zourntos, "A novel distributed privacy paradigm for visual sensor networks based on sharing dynamical systems," *EURASIP Journal on Advances in Signal Processing*, vol. 2007, Article ID 21646, 17 pages, 2007.

[13] Y. Chu and A. Ganz, "A mobile teletrauma system using 3G networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 4, pp. 456–462, 2004.

[14] C. Chigan and V. Oberoi, "Providing QoS in ubiquitous telemedicine networks," in *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom '06)*, pp. 496–500, Pisa, Italy, March 2006.

[15] A. Qureshi, A. Shoeb, and J. Guttag, "Building a high-quality mobile telemedicine system using network striping over dissimilar wireless wide area networks," in *Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS '05)*, pp. 3942–3945, Shanghai, China, September 2005.

[16] G. Cheung, P. Sharma, and S.-J. Lee, "Striping delay-sensitive packets over multiple bursty wireless channels," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '05)*, pp. 1106–1109, Amsterdam, The Netherlands, July 2005.

[17] A. Qureshi and J. Guttag, "Horde: separating network striping policy from mechanism," in *Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services (MobiSys '05)*, pp. 121–134, Seattle, Wash, USA, June 2005.

[18] K. Chebrolu and R. R. Rao, "Bandwidth aggregation for realtime applications in heterogeneous wireless networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 4, pp. 388–403, 2006.

[19] K. Chebrolu and R. R. Rao, "Communication using multiple wireless interfaces," in *Proceedings of the Wireless Communications and Networking Conference (WCNC '02)*, vol. 1, pp. 327–331, Orlando, Fla, USA, March 2002.

[20] D. Zhu, M. W. Mutka, and Z. Cen, "QoS aware wireless bandwidth aggregation (QAWBA) by integrating cellular and adhoc networks," in *Proceedings of the 1st International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine '04)*, pp. 156–163, Dallas, Tex, USA, October 2004.

[21] J. Luo, R. Mukerjee, M. Dillinger, E. Mohyeldin, and E. Schulz, "Investigation of radio resource scheduling in WLANs coupled with 3G cellular network," *IEEE Communications Magazine*, vol. 41, no. 6, pp. 108–115, 2003.

[22] C. Doukas, I. Maglogiannis, and G. Kormentzas, "Advanced telemedicine services through context-aware medical networks," in *Proceedings of the International Special Topics Conference on Information Technology in Biomedicine (ITAB '06)*, Ioannina-Epirus, Greece, October 2006.

[23] HIPPAA, "Health Insurance Portability Accountability Act".

[24] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 162–175, Baltimore, Md, USA, November 2004.

[25] V. Shnayder, B.-R. Chen, K. Lorincz, T. R. F. Fulford-Jones, and M. Welsh, "Sensor networks for medical care," Tech. Rep. TR-08-05, Division of Engineering and Applied Sciences, Harvard University, Cambridge, Mass, USA, 2005.

[26] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," in *Proceedings of the 1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON '04)*, pp. 71–80, Santa Clara, Calif, USA, October 2004.

[27] S.-D. Bao and Y.-T. Zhang, "A design proposal of security architecture for medical body sensor networks," in *Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks (BSN '06)*, pp. 84–87, Cambridge, Mass, USA, April 2006.

[28] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communication Security*, pp. 41–47, ACM press, Washington, DC, USA, November 2002.

[29] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for sensor networks," in *Proceedings of the CADIP Research Symposium*, Baltimore, Md, USA, October 2002.

[30] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom '01)*, pp. 189–199, Rome, Italy, July 2001.

[31] V. Gupta, M. Millard, S. Fung, et al., "Sizzle: a standards-based end-to-end security architecture for the embedded internet," in *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom '05)*, pp. 247–256, Kauai Island, Hawaii, USA, March 2005.

[32] 2003, IEEE Standard for Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs).

[33] July 2004, ZigBee Alliance Document 02130: Network Layer Specification.

[34] S. Dagtas, G. Pekhteryev, and Z. Sahinoglu, "Multi-stage real time health monitoring via ZigBee in smart homes," in *Proceedings of the 21st International Conference on Advanced Information Networking and ApplicationsWorkshops (AINAW '07)*, vol. 2, pp. 782–786, Niagara Falls, Ontario, Canada, May 2007.

[35] W. He and K. Nahrstedt, "An integrated solution to delay and security support in wireless networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '06)*, vol. 4, pp. 2211–2215, Las Vegas, Nev, USA, April 2006.

[36] H. Çam, "A distributed dynamic channel and packet assignment for wireless multimedia traffic," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '00)*, vol. 3, pp. 1131–1135, Chicago, Ill, USA, September 2000.

[37] J. S. Steinberg, S. Zelenkofske, S. C. Wong, M. Gelernt, R. Sciacca, and E. Menchavez, "Value of the P-wave signal-averaged ECG for predicting atrial fibrillation after cardiac surgery," *Circulation*, vol. 88, pp. 2618–2622, 1993.

[38] B. Huang and W. Kinsner, "ECG signal compression and analysis in long-term monitoring," in *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE '99)*, vol. 2, pp. 797–800, Edmonton, Alberta, Canada, May 1999.

[39] B. Aehlert, *ECGs Made Easy*, Mosby, Edinburgh, UK, 3rd edition, 2006.

[40] TINYOS, http://www.tinyos.net/.

[41] D. Seetharam and S. Rhee, "An efficient pseudo random number generator for low-power sensor networks," in *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN '04)*, pp. 560–562, Tampa, Fla, USA, November 2004.

[42] S. Ozdemir and H. Çam, "Key establishment with source coding and reconciliation for wireless sensor networks," in *Proceedings of the 25th IEEE International Performance, Computing, and Communications Conference (IPCCC '06)*, pp. 407–414, Phoenix, Ariz, USA, April 2006.

[43] POWERTOSSIM, http://www.eecs.harvard.edu/~shnayder/ptossim/.

[44] XBOW, http://www.xbow.com/.

[45] R. Rivest, "The MD5 message-digest algorithm," IETF RFC 1321, April 1992, ftp://ftp.rfc-editor.org/in-notes/rfc1321.txt/.

[46] A. Wood, G. Virone, Q. Cao, et al., "ALARM-NET: wireless sensor networks for assisted-living and residential monitoring," Tech. Rep. CS- 2006-13, Department of Computer Science, University of Virginia, Charlottesville, Va, USA, 2006.