# Secure Sensor Data Transmission over Wireless Cellular Networks

George M. Stamatelos

Electrical & Computer Engineering Department

Democritus University of Thrace, Xanthi 67100, Greece, gstamate@ee.duth.gr

## Abstract

*Significant effort has been recently devoted to research and development of sensor networks for a wide range of possible applications. Here we focus on the design of a biosensor-based, early-warning system that can be used to detect bio-threats and subsequently relay securely this information - through a cellular network and its communications capabilities - to public health surveillance centers for appropriate processing. As such, it represents an alternative approach to population vaccination against specific viruses and biological threats. Issues involving increased security of communications and network dimensioning are addressed in the above context.*

### 1. Introduction

Sensor networks are currently proposed in the relevant literature for a wide range of applications including military surveyor networks and self-regulating mechanisms for civil applications. Generally speaking, self-organizing sensor networks may be built from autonomous sensor nodes that may spontaneously create a dynamic-topology network. Such a network can adapt to device failure or malfunctioning, allow for mobility of sensor nodes, and react positively to dynamically varying network conditions. The sensor network that we propose here is different in the sense that, for both its organization and communications needs, it takes advantage of the widely existing cellular network infrastructure (e.g. GSM, IS-95 etc.).

Also, most of the wireless sensor networks in the literature (see for example [1], [2]), unless capable of exploiting radio frequency energy, rely on self-powered sensors with limited lifetime. In our proposal micro-fabricated biosensors such as those described in [3] are integrated into mobile devices and therefore make use of the mobile phones (rechargeable) power supply, for both their functionality and communication needs. They target the detection of one or several viruses classified as biological threats.

Continuous measurements[1] of the environment around the biosensors – along with location information – are captured and sent periodically in the form of SMS messages (Short Message Service) in a GSM-based PLMN (Public Land Mobile Network or generally a second or third generation wireless cellular network e.g. IS-95 in the appropriate text format). The content of these messages is encrypted- as described in the next sections and [5] - for security purposes, using a strong encryption algorithm (for example AES[2] or even the older triple-DES). The encryption process is of crucial importance for both the authenticity of the collected sensor data, as well as, the system's integrity and its protection against malicious third-party attacks. Aggregation and processing of the sensor data is subsequently done in central locations that construct synthetic views on the existence (or absence) of specific biological threats.

The organization of this paper is as follows. Section 2 describes the basic architecture for the flow of biosensor data, through the cellular network to central locations where processing of the collected information takes place. Section 3 addresses the security aspects of the information transfer as well as, the cryptographic protection of the biosensor data and the system integrity. Section 4 provides simulation results of a possible sensor

[1] For minimum-cost deployment the system can be designed to send data only when the detection values are non-zero. Periodic measurements (of a predefined frequency) along the mobile path is another alternative.

[2] AES, DES stand for the Advanced and Data Encryption Standard Standard (see [4] ).

*Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6047*
*http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6047*

network architecture followed by our conclusions in section 5.

## 2. Network architecture and data flow

Mobile-originated short message transfer of the biosensor measurements takes place with the actual data decrypted at the participating message processing centers - MCs or SM_SCs (Short Message Service Centers) in the GSM terminology- as shown in Figure 1 below. In an alternative approach the biosensor data are decrypted at the first level processing centers (Health Alert Processing Centers) where their validity is also tested against possible sensor malfunctioning.

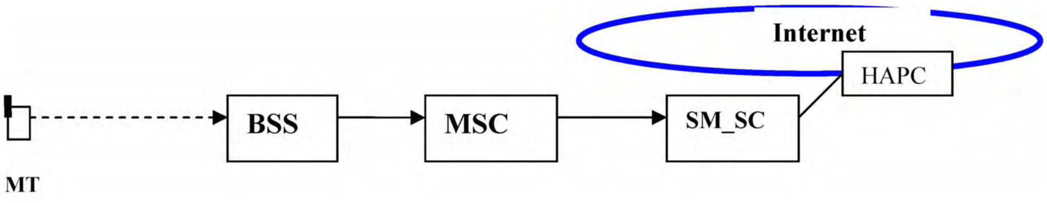

**Figure 1. Biosensor data flow from mobile (MT) towards SM_SC/ HAPC over a GSM network.**

A number of these message centers (MCs) are distributed in the periphery of the supporting MSC network. As also shown in Figure 1 above, MCs can be connected – via secure Internet (VPN) or leased line connections for example – to the health alert processing centers (HAPCs) where aggregation of sensor data / location information collection and bio-sensor information processing from the participating MCs takes place.

These HAPCs - besides organizing data into certain structures (using for example the X.500 format) and rejecting invalid biosensor data[3] - are responsible of constructing (in a hierarchical manner) a composite view of the biosensor information for an area of coverage falling into their responsibility (Figure 2).

Flow of sensor data is from the lower level to the higher hierarchy levels. At the highest level (third level in the hierarchy in Figure 2 below) a general view of the existence or absence of specific biological threats is constructed, potentially covering a very significant portion of the country's population. Regarding the total generated traffic load from the active biosensor units, it is a function of both the number of deployed biosensors as well as, the defined frequency of message emission. In terms of addressing, the SMS messages with the biosensor measurements could be distinguished from common SMS messages either via specific central processing (e.g. HAPC) phone numbers or by inclusion of header information (see ref. [6]).

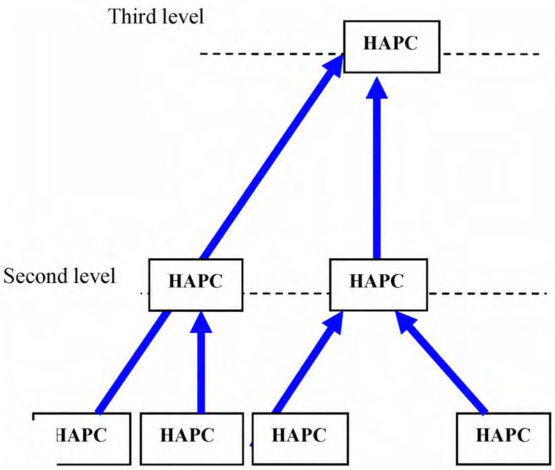

**Figure 2. Hierarchical structure of health alert processing centers.**

[3] Invalid sensor data detection could be based for example on observing sensors reporting constantly high values independently of mobile location or sensor data that are not confirmed by any neighboring sensors.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6047
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6047

Along with sensor data, location information of the mobile[4] terminal (MT) is also collected using one of a variety of location techniques of variable accuracy. CellID for example is a technique for locating a user according to the base-station with which their mobile has established a session. By looking up the identity of the base-station the geographical location of the mobile can be determined.

With assisted global positioning service (A-GPS), the network provides GPS data to the mobile phone in order to expedite the calculation of its position from the GPS signals it can receive. A third well-known scheme is Enhanced Observed Time Difference (EOTD) that compares the arrival time of network signals at the mobile with the arrival time at network measuring devices, and inputs these measurements into a triangulation calculation as shown in the figure below:

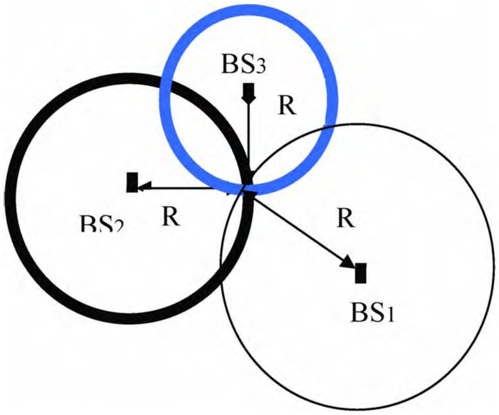

**Figure 3. EOTD triangulation calculation, R1, R2, R3 the distances from the respective BSs.**

### 3. Secure SMS transmission

In this section we address the issue of secure information transport between the biosensor unit and the HAPC. Both authentication and authorization phases need to be confirmed before the actual encryption of data flows between the two communicating sites. At the end of this process the two parts should have established a secret key that is further used for the "symmetric" (DES or AES-based) encryption of the biosensor data, as shown in Figure 4.

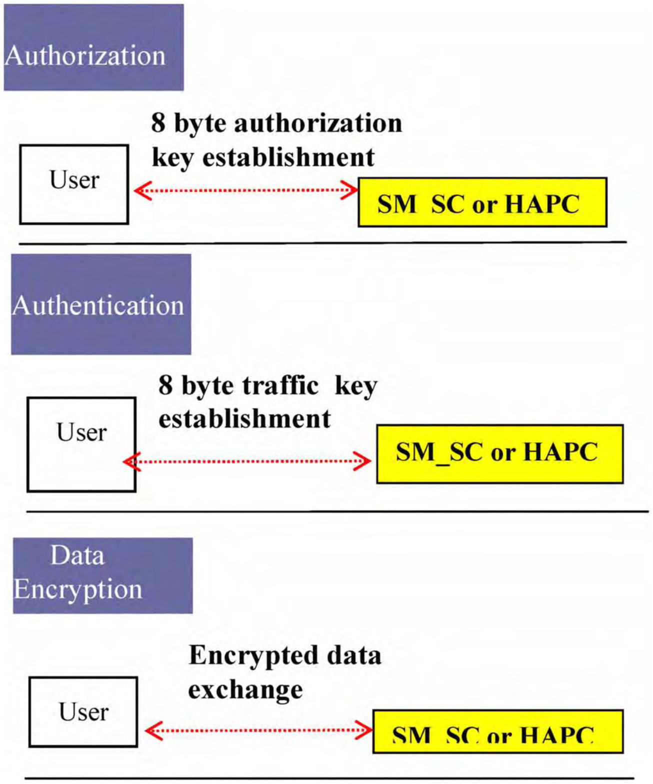

**Figure 4. Authentication, Authorization, and Encryption processes.**

User (sensor) authentication/ authorization are processes that need to be established before the encryption of sensor data and the actual transmission between the two sites. During the first phase, authorization takes place by having the user (MT) submitting a message request to HAPC requesting an authorization key. In this message the user (MT) includes its public key, which consists of a 96 byte modulus and a 3-byte exponent. The HAPC responds by encrypting an 8-byte authorization key (using for example RSA software and the public key of the user). The mobile terminal (MT) decrypts the authorization key using RSA (and its private key).

Now both sides have the same authorization key; they use it to create three additional keys: the key encryption key (8 bytes), the upstream message authentication key (20 bytes originating from MT) and the downstream message authentication key (20 bytes with destination the MT).

[4] The location of the mobile corresponds also to the location of the biosensor

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6047
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6047

In the second phase the MT submits a message/ request for a traffic key (that contains an HMAC digest , i.e. a hash-based Message Authentication Code (MAC) which is a function of a variable length input and a key in order to produce a fixed length output, that is, a type of electronic signature that authenticates the user). HAPC (or SM_SC) authenticates the request (using SHA-1 and the respective key (i.e. upstream message authentication key that has been established during the previous phase) and if it checks and the MT authentication is successful as well, then HAPC (or SM_SC) encrypts an 8-byte traffic key using DES[5] and sends it back to the MT along with its own HMAC digest.

Now that both sides have established the same (secret) traffic key, actual data encryption begins and secure data flows can be exchanged between MT and SM_SC (or MT ← → HAPC). Traffic key reestablishment should also take place in regular time intervals for purposes of increased security. The messages that are exchanged should not exceed a certain limit (140 bytes in GSM networks). If for any reason, the required information exceeds this threshold, concatenation of messages can also be used instead (as described in reference [7]).

## 4. Network Simulation Results

A possible network architecture for the transport of sensor messages is shown in figure 5 below. We assume that biosensor data in the form of periodic (Constant Bit Rate) packet streams enter – through the path BSS/MSC/SM_SC/HAPC – the tethered network segment (Source 1 for example) to be eventually forwarded (through routers R1 and R2) to the central processing unit (Destination 1 in the tethered segment topology of Figure 5) where collection/ processing of all biosensor data takes place.

We have used the well-known NS-2 simulator [8] to assess the performance of the tethered network segment (with number of sources n=10 in Fig. 5) in terms of observed throughput/delay/loss parameters.

The generation of biosensor measurements is modeled as a periodic process. Higher priority (HP) is assigned to the transfer of CBR biosensor data (periodic UDP flows of small size packets of 160 bytes long from Sources 1-5 to Dest 1) relatively to other "interfering" lower priority FTP applications (using TCP Reno [9] transport, Sources 6-10 to Destinations 2-6, respectively). The line capacity between Source i and R1 is set to 2 Mb/s (with propagation delay of 10 ms), R1 to R2 is 2 Mb/s (with propagation delay of 10 ms) and R2 to Dest i is set to 4 Mb/s (with propagation delay of 10 ms).

Simulation runs last 400 sec (for each point in the figures below obtained by gradually increasing the packet generation rate of CBR sources, from 0.16 Mb/s to 2 Mb/s).

End –to-end throughput values are shown in Figure 6 to increase for the bio-sensor data traffic (as we virtually increase the frequency of message generation) whereas the respective throughput of the low priority FTP flows steadily decreases reaching zero levels at the point where the bottleneck's link capacity is used to carry exclusively high-priority traffic.

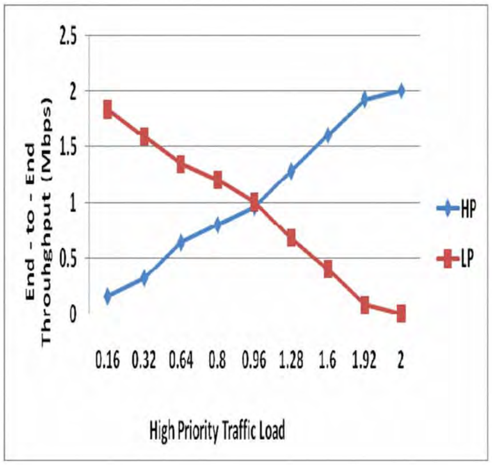

**Figure 6. End-to-end throughput values for high priority (HP CBR) / low priority FTP traffic (LP).**

The same behavior – that is, the effective protection of the high priority traffic - is maintained in the packet delivery ratio results shown in Figure 7 below. It is observed that through the implemented Differentiated Services (DiffServ) approach, when the traffic load from all the high priority sensor data sources saturates the capacity of the bottleneck (2 Mb/s link between R1 and R2 routers), effectively all low priority (FTP traffic) packets are discarded.

[5] A 16-byte key is generated if AES (Advanced Encryption Standard) is used for data encryption.

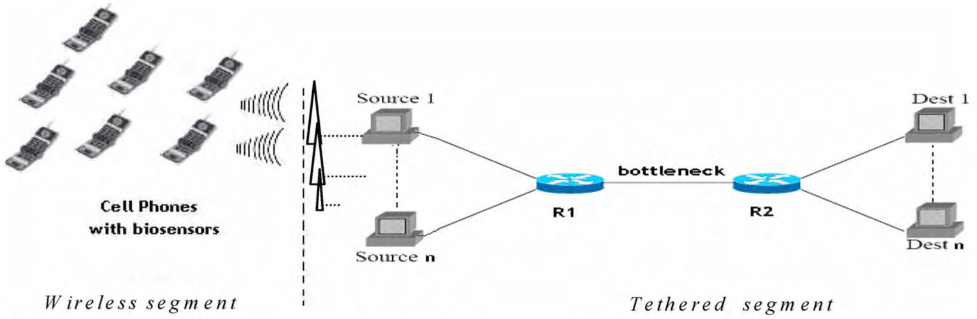

**Figure 5. Simulation network topology – wireless and tethered network segments.**

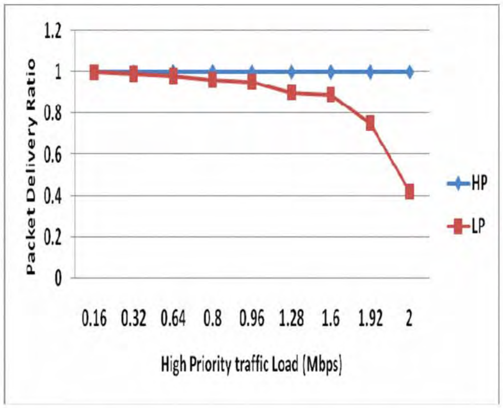

**Figure 7. Packet delivery ratio values for HP and LP traffic as a function of the sensor data load.**

The end-to-end average delay for both types of traffic is shown in Figure 8. Again, near the saturation point, the average delay of the high priority traffic is maintained around 40 ms whereas the respective values for the low priority traffic increase exponentially as shown in the figure below.

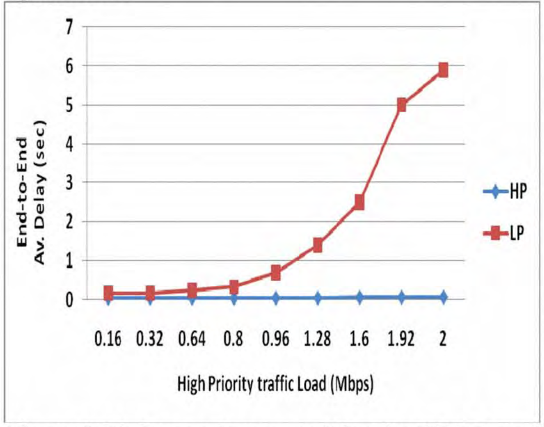

**Figure 8. End-to-end average delay for HP,LP traffic.**

## 5. Conclusions

Addressing public safety concerns by means of early risk identification systems is a very challenging task, imposing difficulties due to the magnitudes involved. In this context, the proposed early-detection network based on micro-fabricated biosensors offers significant advantages for the confrontation of bio-threats, mainly because of providing the possibility of detecting and communicating securely the onset of a virus incubation period.

We argue here that a combination of biosensor capabilities with the wide area coverage of a cellular system may represent a viable alternative to wide population vaccinations, worthwhile looking into it carefully.

## 6. References

[1] D. Culler, D. Estrin, M. Srivastava, "Overview of Sensor Networks," IEEE Computer, 2004, pp. 41-49.

[2] I. Akyildiz, et. al.,"A survey on wireless sensor networks", IEEE Communications Magazine, 2002, 40(8):102–114.

[3] C. Aston, "Biological Warfare Canaries", IEEE Spectrum, Oct. 2001, pp.35 – 40.

[4] B. Schneier, "Applied Cryptography", Wiley 2003.

[5] US Patent 7,076,657, G. Stamatelos V. Koukoulidis, "Use of short message service (SMS) for secure transactions".

[6] US ap. Patent, 20030123669 G. Stamatelos V. Koukoulidis, "Public health threat surveillance system".

[7] 3GPP TS G4.11.v 7.1.0 , Feb. 6, 2001. "Digital Cellular Telecommunication System" (Phase 2+): Point – to –Point (PP) Short Message Service (SMS)".

[8] The ns-2 Network Simulator http://www.isi.edu/nsnam/ns/

[9] V. Jacobson, "Congestion Avoidance and Control", ACM SIGCOMM 1988, August 1988.

*Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6047*
*http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6047*