INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

SECURITY ON MEDICALWIRELESS SENSOR NETWORKS: A SURVEY

Ghasem Farzaneh[1], Ali Rahnamaei[1]

[1]*Department of Computer Engineering, Ardabil Branch, Islamic Azad University, Ardabil, Iran*
Author Correspondence: ghasemfarzaneh2008@yahoo.com

Abstract: - Wireless technology is fast becoming a very important tool for all aspects of communication. An area that lacks a strong implementation for wireless communication is the medical field. Wireless systems could be used by clinicians to be better able to diagnose and monitor patients. The reason behind the lack of adoption in healthcare is due to the need to meet the legislated and perceived requirements of security and privacy when dealing with clinical information. The current methods of wireless authentication are investigated and an existing issue in mobile networks is described and solved with two novel solutions; one solution within GSM and the other within UMTS. Strong authentication protocols are developed based on the existing wireless protocols, while using minimal messages and symmetric operations to limit resource utilization to meet the needs of the healthcare environment. To ensure the quality of the protocol a BAN (Burrows-Abadi-Needham logic) analysis is performed which verifies that the desired goals of the protocols are appropriately met within the results analysis. The developed security protocol is shown to be secure, uses minimal messages to maintain efficiency and meets the legal requirements to be used in medical wireless sensor networks.

Keywords: Medical Wireless Sensor Networks, Authentication, Integrity, Key Agreement, BAN Analysis, Mobile, Security, Privacy, HIPAA, and PIPEDA.

1. Introduction

Technological innovations for communication and computing have been advancing at an accelerated pace. The ability to co-ordinate and communicate between many devices by using wireless communication has had a major impact in many areas of life. One area that has seen slow advancement is medical care. There are many concerns about the security and integrity of the information created and stored in the systems that are being developed to help meet the needs of clinicians and patients. Patient privacy and safety are of major concern when applying many of the new innovations in wireless communication to the problems faced by the medical community. The general public is concerned about how their medical information is stored, transmitted and cared for. Clinicians are concerned about the quality and integrity of the medical data they receive. To help alleviate the perceived issues of applying wireless technology to monitor patients, it is worthwhile to investigate existing security issues in wireless networks as well as how those issues have been resolved. By applying the experience gained from wireless deployments it will be possible to address the concerns and requirements of clinical systems, to ensure the safety of patients and staff. Before wireless technology can be applied to the clinical environment, which will bring many benefits and advantages to clinical care, the security

issues need to be addressed. The ability to remotely track patient information will allow clinicians a more robust picture of patient health. The extended time that patient information can be gathered will increase the understanding of the results of medical treatments and allow for stronger refinement of those treatments to create better results overall or tailored treatments for each patient. The technology will afford clinicians the ability to understand if a patient is in stable or in declining health over a long period of time. The remainder of this article is organized as follows: section 2 provides a broad background on many of the requirements, implications, and needs of medical wireless sensor networks (M-WSN) as well as information pertaining to security of wireless communication. In section 3 we discuss authentication in existing 802.11 and mobile networks and the issues faced by those networks as they have adapted to new security challenges. A scenario on how an M-WSN would be used is discussed as well as how the authentication of the system is achieved and a formal verification that the authentication achieves the desired results are in section 4. section 5 discusses other privacy concerns and how they may be addressed. Chapter 6 concludes this thesis and offers future research directions and suggestions.

2. Medical Wireless Sensor Networks (MWSN)

Wireless Sensor Networks will have a very large impact on many aspects of society from military applications to common household appliances. The application of WSN to the field of medicine will have widespread consequences in the gathering of medical information and giving a more robust picture of patient health. Sensor networks can give real-time information and telemetry to the clinicians that require the information to properly respond to medical situations and emergencies. A MWSN can track many different aspects of the patient including movement inside their home, their temperature and other bio-medical information such as oxygen saturation. The telemetry will help reduce costs for healthcare facilities by allowing patients to be remotely monitored instead of being in a facility for observation. There are a few different frameworks based on the Telos Mote[5] and Mica[6] Sensors. These frameworks generally use TinyOS [7] to efficiently manage and utilize their resources with many different deployment strategies to meet the differing needs of modern healthcare. Along with sensor information, there is a very real possibility of medication being delivered in minute doses to patients based on information gathered from medical sensor networks. The delivery of the medication would be controlled by wireless communication. When the information gathered from an MWSN reaches this level of integration with the medical care of patients, it is imperative that all communication be very secure with high integrity and availability so that no mistakes can occur and to be certain that the medication needed is the medication delivered to the patient when needed. The types of sensor networks gathering the medical telemetry that can be used in the healthcare problem space are body sensor networks that are affixed to the patient or implanted inside the body and environmental sensor networks that gather information from the environment and are not physically connected to the patient and are usually stationary. We describe both types of sensor networks in the next two sections.

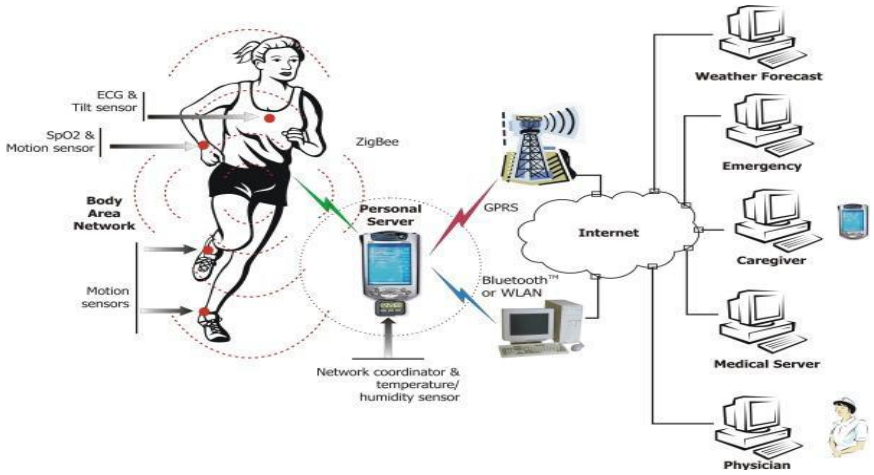

Figure 1: healthcare application using wireless sensor network

2.1 Body Sensor Networks

The sensors are applied directly to the body and monitor patient vital signs. The sensors will gather the information from the body and send it to clinicians for understanding and monitoring. The CodeBlue framework presented by V. Shnayder, et al. [8] shows a decentralized integrated MWSN for use in a clinical setting that will allow clinicians to query patient sensors to send vital information. The telemetry devices they use to collect data include a pulse oximeter, two-lead electrocardiogram, and a specialized motion-analysis sensor. They have built routing protocols to allow a clinician device to be able to query and receive data from these sensors while at a remote location in the medical facility. The CodeBlue framework lacks security and data protection. B.Sarikaya, et al. [9] integrate electroencephalography (EEG) sensors into the CodeBlue framework. There are other frameworks that have encryption and integrity but lack authentication or key agreement such as Kumar, et al. [10] who have built a sensor system for monitoring patients; their example monitors Electrocardiograph (ECG) information. To ensure confidentiality of the data, they have used the Ping-Pong [11] encryption algorithm with the Ping-Pong MAC to ensure integrity. They proceed to develop a framework in [12] based on the original paper where they describe an application that allows the sensor information to be presented to clinicians in a human usable format. Waluyo, et al. [13] have developed a centralized framework that has a personal digital assistant (PDA) or other powerful computing device as a sensor gateway. They have built the functionality for data collection as well as command and control within their network which is built on TinyOS on the sensors with a Java framework on the PDA. They have applied the SkipJack [14] encryption algorithm to their communication to ensure confidentiality. There is no method of Authentication and Key Agreement (AKA) as they have a single pre-distributed key for all devices. A home network for health monitoring is proposed by Singh, et al. [15] which relies on stationary cameras, a PDA, body sensors, and home health controller system. This will then send the clinical information over the internet to a medical center. They use an Encrypted Key Exchange (EKE) [16] protocol for key distribution as well as a Key Distribution Center (KDC) to limit the impact of losing the PDA as a core device in the network. When establishing keys between body sensors the EKE uses user secure environmental values (SEV) such as Inter-Pulse-Interval (IPI) or Heart Rate Variance (HRV). Diffie-Hellman based EKE (DH-EKE) described in their work is used to establish a session key, SEV is used as the Encryption in EKE. They show how this uses fewer resources than Elliptic Curve Cryptography (ECC). PDA authentication uses KDC with a multiple server protocol (each of the cameras). The user enters a password into the PDA. This password is used as the encryption in the DH-EKE to authenticate the PDA against the cameras. All of the cameras then authenticate against the PDA sending secure information allowing the PDA to authenticate the body sensor. As long as a minimum number of cameras return the proper values then the PDA is authenticated against the body sensor.

2.2 Environmental Sensor Networks

Environmental sensors are placed within an environment to track information on the patient and the environment which gives a holistic view of all conditions that the patient may experience. An example is the stationary cameras previously mentioned in a home network for health monitoring proposed by Singh, et al. [15]. Some sensors already exist in the home such as carbon dioxide and carbon monoxide sensors. Sensors can be added to the bed to monitor movement of bedridden patients to give information that would help clinicians reduce the occurrence of bedsores. Infrared and other types of sensors can be used in the environment to monitor patient bio-metric data without needing physical contact with the patient.

2.3 Key Agreement in Sensor Networks

Key agreement is required in a secure network to allow devices to begin to communicate securely and with integrity. Du, et al. [21] describe a methodology for an asymmetric pre-distribution key management scheme in a Heterogeneous sensor network. Their design has pre-distributed key pools to the sensors that allows for high probability of key agreement between sensor nodes. The nodes can therefore authenticate against each other by use of the pre-distributed keys. Camtepe, et al. [22] also propose a probabilistic key distribution methodology

to increase the likely-hood that two sensors will be able to authenticate each other and proceed to communicate securely. The proposed security framework for wireless medical sensor networks in Morchon, et al. [23] relies on cryptographic keying material, a lightweight digital certificate linked to the keying material and a security policy. This system is used to enable distributed key agreement by means of the multidimensional secure key establishment scheme and cryptographically enforced access control. Each node has keying material related to the main security domain as well as other keying material related to each of the sub-domains to which it has access. The design allows for quick and easy agreement between the medical devices such as a PDA and the sensors on the type of access allowed by matching the keying material.

2.4 Encryption and Integrity in Sensor Networks

The limited resources in sensor networks require the design of the security to be limited. To achieve confidentiality, Malasri, et al. [19] use the RC5 [24] encryption algorithm and to achieve integrity in their communication they use the SHA-1 [25] algorithm. Waluyo, et al. [13] use the SkipJack encryption algorithm to secure the information sent in their framework from passive eavesdropping. They do not have any integrity algorithms to ensure the quality of the communication and they do not have any protections against active attacks. The single key used on all devices will allow one compromised device to have full access to all information on their MWSN. The Ping-Pong and Ping-Pong-MAC algorithms used by Kumar, et al. [10] meet both of these requirements of confidentiality and integrity allowing the sensor to use similar algorithms to reduce the overhead in both of these operations. There are many tools used in security to achieve these goals such as stream ciphers, block ciphers and cryptographic hash functions. Due to the limited resources available to sensor nodes it may be appropriate to use stream ciphers to secure the communication between nodes since they generally use less overhead and can easily be implemented in hardware. Ping-Pong, RC4, A5/1 and A5/2 are stream ciphers that are used to protect communication. RC4 is the algorithm used in WEP and it is also in active use by many websites such as Gmail, Amazon, and RBC. A5/1 and A5/2 are encryption algorithms used in GSM communication but these algorithms have serious flaws. Block Ciphers generally require more resources than stream ciphers but there are many advantages of using block ciphers. Block ciphers are the most active area of symmetric encryption research and they provide many different modes of securing the information that have been accepted by the National Institute of Standards and Technology [26]. One mode of operation is Cipher Block Chaining (CBC) which reduces the chance of using a dictionary attack on the cipher text as each input block is XORed against the previous block of cipher text. Other modes of operation that are very useful and allow the block cipher to act as a stream cipher are Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR). Counter mode has the added advantage of being able to be decrypted in parallel. Due to the increased complexity of block ciphers most cannot be easily implemented in hardware but the AES block cipher is able to be implemented in hardware. Hash functions have many applications in security and allow for simple methods of ensuring integrity. Cryptographic hash functions take an input message and create a pseudorandom output message digest that is easy to compute given the message but it is infeasible to generate a message given the hash digest. It is also infeasible to modify a message without changing the hash or to find two different messages with the same hash. These properties make hashing a useful tool for integrity and for deriving pseudorandom keys.

3. Authentication for Medical Wireless Sensor Networks

Authentication is the first step in ensuring the safety, privacy and security of user information in a medical wireless sensor network system. The following sections will detail a scenario on usage of an M-WSN and how each component will authenticate to the secure system. Please note that the scenario will have areas that are numbered for future reference during discussion of our protocol. The communication routing between the smart control node and the clinical server can go over wireless and physical networks, as well as the internet. The smart control node will already have been connected wirelessly to the network in the hospital using their supported Wi-Fi protocols. The clinical staff will establish a connection to the clinical server to select the patient for the smart control node to monitor which is how this protocol is used to support the security requirement mentioned. The SmartId and KSmart are preloaded onto the smart control node before distribution to the clinical environment. The protocol developed for authentication for the smart control node creates an

understanding between the smart control node and the clinical server of shared keys for authentication and integrity to be used for communication. The original protocol allows a clinician to attach a patient to the smart control node for collection of telemetry. The second protocol allows the patient telemetry to be sent from the smart control node to the clinical server in a secure manner and for command and control instructions to be sent in either direction. The BAN analysis of the protocols shows that mutual authentication and key agreement is achieved for both of these protocols. We have limited messages and use hashing functions to limit the resource usage. The protocol developed for the sensor nodes allows the smart control node to communicate securely with the sensors to send or receive information. Mutual authentication and key agreement is achieved between the smart control node and the sensor node while using the clinical server as a mediator. The re-authentication allows for the sensors to communicate securely with the smart control node even in the absence of a connection to the clinical server. All of the protocols use minimal resources and messaging to achieve the desired results as can be seen with the BAN analysis. Patient privacy is of the utmost concern in any clinical system. Clinicians will try to gather as much data as possible since any minor facet of a patient's life can have an impact on their health. To have a full picture and be able to fully analyse the problems a patient is having, health care providers would prefer to have knowledge of even the most minor of details Healthcare providers try to collect and store the most intimate details of our lives to be able to properly diagnose any health issues a patient may experience. This information could be put to many nefarious uses if it gets into the hands of the wrong people. To limit patient exposure to black mail and other undesired effects of the release of this information it is required that patient privacy be maintained. Patient Privacy must be maintained to limit the release of this private information to only those clinicians directly responsible for the care of a patient. This implies that the sensitive information will not be released to clinicians not responsible for the care of the patient or to any outside party that should not have access to or knowledge of the sensitive information. Both the Canadian and American governments have tried to tackle the issue of patient privacy by crafting laws that apply to the care and control of patient information. As mentioned Canada has developed the Personal Information Protection and Electronic Documents Act and the United States has enacted the Health Insurance Portability and Accountability Act. This legislation calls for the utmost care to be taken with patient/personal information. When considering new advances in clinical care and with the advent of wireless technology, the amount of information that is collected by clinical providers is growing massively. It is now possible for many different methods to breach patient privacy. A passive observer can simply record the information a patient system is transmitting to discern the location of the patient. If the information is transmitted without care for the confidentiality of the information then the observer can have direct access to that information. Active attacks on privacy can come from many directions. The wireless communication medium is particularly attractive to attack. Other active attacks on patient privacy can be carried out by employees and clinicians related to the health care provider that abuse their privileges to discover the personal information of a patient for which they do not provide care. These types of attacks need to be addressed by defining the types of privacy that should be afforded to the patient.

There are potential large impacts for sensor networks applications in e-healthcare scenario [6]. These can be realized through real-time, continuous vital monitoring to give immediate alerts of changes in patient status. Also, the Wireless Body area Network WBAN operates in environments with open access by various people such as hospital or medical organization, which also accommodates attackers. The open wireless channel makes the data prone to being eavesdropped, modified, and injected. Many kinds of security threats have been existed, such as unauthenticated or unauthorized access, message disclosure, message modification, denial-of-service, node capture and compromised node, and routing attacks, etc. Among which two kinds of threats play the leading role, the threats from device compromise and the threats from network dynamics which are analyzed detailed in Table 1 [4]. The patient-related data if not well kept or just stored in one node, could be lost easily due to the device compromise or network dynamics.

Table 1. Two Main Kinds of Threats in WBAN

Device Compromise	Network Dynamics
Sensor nodes in a WBAN are subjected to compromised, as they are usually easy to capture and not temper-proof. If a whole piece of data is directly encrypted and stored in a node along with its encryption key, the compromise of this node will lead to the disclosure of data.	The WBAN is highly dynamic in nature. Due to accidental failure or malicious activities, nodes may join or leave the network frequently. Nodes may die out due to lack of power. Attackers may easily place faked sensors in order to masquerade authentic ones, and could take away legitimate nodes deliberately.

4. Medical Emergency Detection in Sensor Networks

The capacity of the US healthcare system has not kept pace with the growing demand for emergency and trauma care. A majority of urban Emergency Departments (EDs) today operate at or over capacity [American Hospital Association 2005], patients are left under-monitored [Coalition for American Trauma Care 2006], and fatalities due to the lack of monitoring have already occurred [CNN 2006; MSNBC News 2006; Stark 2006]. Furthermore, when disasters occur, the surge of patients can quickly overwhelm the already overcrowded care facilities. Thereby, an approach that automates the patient monitoring process has the potential to greatly improve the efficiency of patient flow, increase the volume of patients treated and discharged, and improve the quality of care both on a daily basis and during disasters. With this need in mind, we present MEDiSN, a wireless sensor network for automating the process of patient monitoring in hospitals and disaster scenes. MEDiSN consists of multiple Physiological Monitors (PMs) which are batterypowered motes equipped with sensors for measuring patients' physiological data (e.g., blood oxygenation level, pulse rate, electrocardiogram (ECG), etc.). PMs temporarily store collected measurements and transmit them after encrypting and signing them. Unlike previous systems (e.g., CodeBlue [Malan et al. 2004]) in which PMs also relay data, the MEDiSN architecture incorporates distinct Relay Points (RPs) which self organize into bidirectional wireless trees connecting the PMs to one or more Gateways. Traffic flowing in both directions is protected using hop-by-hop retransmissions that counter the effects of packet collisions and corruptions. The division of functionality between acquiring and relaying data enables PMs to achieve consistent, predictable behavior and low energy consumption, while allowing us to engineer the system to provide superior end-to-end service. Specifically, while PMs can be mobile, the RPs have pre-determined, fixed positions that allow us to provision a high-quality wireless backbone. Furthermore, because PMs are not responsible for relaying traffic, they can aggressively duty cycle their radios to reduce energy consumption. On the other hand, duty cycling is not an option for RPs as they are always busy forwarding packets. Nonetheless, RPs will use the electricity grid in hospital deployments, while in disaster events batteries can power RPs for multiple days. We evaluate MEDiSN's performance through extensive experiments in simulated environments, two indoor testbeds, and multiple pilot hospital deployments. From a networking perspective, we show that dynamically adjusting the maximum number of retransmissions the RPs attempt and computing the optimal inter-packet intervals can increase the system's capacity by 50% and reduce end-to-end delay by threefold. Moreover, properly engineering the RP backbone can increase the packet delivery ratio up to threefold as well. Additionally, we show that aggregation, in which RPs gather multiple small PM messages to maximum length packets, can increase the total number of PMs supported by 30%, while achieving 90% delivery ratio. Results from indoor testbeds indicate that the performance of the actual system accurately matches the simulation results. Using testbed results we also show that MEDiSN outperforms CodeBlue both in terms of delivery ratio for the same number of PMs and in terms of the maximum number of supported PMs. Finally, experimental results suggest that the two-tier routing hierarchy combined with the RP selection scheme allows MEDiSN to perform well even with multiple mobile PMs. We have deployed MEDiSN in multiple IRB-approved clinical studies at the trauma center of the University of Maryland Medical Center and the Johns Hopkins Hospital Emergency Department. These deployments proved that MEDiSN can effectively retrieve data from multiple mobile PMs despite RF-challenging environments with multiple occlusions and considerable interference. Moreover, these studies showed that MEDiSN delivers vital signs measurements that are statistically identical to those generated by (wired) patient monitors commonly used in clinical practice.

5. Conclusions

The application of wireless communication to the medical field will have many beneficial and far reaching impacts on the way healthcare is delivered. The legislated requirements relating to the handling of clinical and personal information require that security be at the core of any system developed for a clinical application. HIPAA in the United States of America and PIPEDA in Canada are two examples of government legislation that have a direct impact on the way that health and personal information can be collected and transmitted. Major issues are the confidentiality and integrity of the information collected and transmitted which requires a strong method of authentication and key agreement. To address these privacy and legislated issues authentication, key agreement, encryption, and integrity hashing are required technologies that need to be implemented in any Medical Wireless Sensor Network. The existing wireless authentication frameworks are investigated; these networks are currently deployed and have undergone extensive testing and have withstood a great number of real world attacks. The authentication in WEP, WPA and WPA2 are discussed, showing the

problems that existed in the older protocols and how they were overcome by the next generation of technology and protocols. The issues in WEP are not related to the encryption algorithm but the implementation of the protocol that cause the weaknesses. We also investigate the mobile wireless network protocols, showing the different evolutionary constraints on the systems that are deployed and developed. A major issue with the integration of GSM and UMTS security protocols is revealed and two solutions are proposed showing how to increase the security by using simple hashing techniques. The information gained from examining the existing wireless protocols gave a foundation for the protocols designed in this thesis. The protocols are designed to achieve mutual authentication and key agreement for secure communication between the smart control node, clinical server and sensor nodes use minimal messages. The protocols also avoid public key encryption due to the increased processing and resources required to implement public key protocols. The protocols are analyzed using BAN analysis showing that they are secure and achieve the desired result of mutual authentication and key agreement. Other aspects of privacy are then investigated with possible methods of addressing the privacy issues. Location privacy is of large concern and will need to be addressed and the MIST and TOR protocols meet some of the needs of location privacy. The issues of identification and information privacy are also discussed with an overview on possible solutions to address those problems. The protocol developed is an excellent foundation for the implementation of wireless sensors for healthcare. This thesis addresses the legal requirements of privacy required by both Canada and the United States. The protocols developed will allow for the application of sensors to many different areas of clinical telemetry.

5.1 Future Work

The further development of the protocols presented in this thesis, to meet the growing privacy needs of both patients and clinicians, is a worthwhile avenue of research. The intent of this researcher is to attempt to create a practical working product for use in clinical environments and to begin to properly leverage wireless communication within the healthcare environment.

REFERENCES

[1] U. S. Government, “Health insurance portability and accountability act,” 1996. [Online]. Available:http://www.gpo.gov/fdsys/search/pagedetails.action?granuleId=CRPT104hrpt736&packageId=CRPT-104hrpt736.

[2] G. of Canada, “Personal information protection and electronic documents act, “April 2000. [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/P- 8.6/index.html.

[3] G. of Ontario, Canada, “Personal Health Information Protection Act,” 2004. [Online]. Available:http://www.elaws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm.

[4] G. of Ontario, Canada, “Freedom of Information and Protection of Privacy Act,” 1987.[Online].Available:http://www.elaws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm.

[5] J. Polastre, R. Szewczyk, and D. Culler, “Telos: Enabling ultra low power wireless research,” in Proc. 4th Int. Symp. Inf. Process. Sensor Netw., Los Angeles, CA, 2005, pp. 364–369.

[6] MICA Sensors, http://gyro.xbow.com/Products/Wireless_Sensor_Networks.htm.

[7] P. Levis et al., “TinyOS: An operating system for sensor networks,” in Ambient Intelligence, W.Weber, J. Rabaey, and E. Aarts, Eds. Berlin: Springer, 2005, pp. 115 148.

[8] V. Shnayder, B. Chen, K. Lorincz, Thaddeus R. F. Fulford J. and M.Welsh, Sensor Networks for Medical Care, Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University,2005,ftp://ftp.deas.harvard.edu/techreports/tr 2005.html.

[9] B. Sarikaya, M. A. Alim, and S. Rezaei, “Integrating wireless eegs into medical sensor networks,” in Proceedings of the 2006 international conference on Wireless communications and mobile computing, ser. IWCMC ’06. New York, NY, USA: 99 ACM, 2006, pp. 1369–1374. [Online]. Available: http://doi.acm.org/10.1145/1143549.1143823

[10] P. Kumar, Y.-D. Lee, and H. Lee, “Secure health monitoring using medical wireless sensor networks,” in Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on, Aug. 2010, pp. 491 – 494.

[11] H. Lee and K. Chen, “Pingpong-128, a new stream cipher for ubiquitous application,” in Convergence Information Technology, 2007. International Conference on, nov. 2007, pp. 1893 –1899.

[12] M. Sain, P. Kumar, and H. J. Lee, "Secure authentication and communication in ubiquitous healthcare middleware," in Advanced Communication Technology (ICACT), 2011 13th International Conference on, Feb. 2011, pp. 173 –178.
[13] A. B.Waluyo, I. Pek, X. Chen, and W.-S. Yeoh, "Design and evaluation of lightweight middleware for personal wireless body area network," Personal Ubiquitous Comput., vol. 13, pp. 509–525, October 2009. [Online]. Available: http://dx.doi.org/10.1007/s00779-009-0222-y
[14] [N. S. Agency, "Skipjack and kea algorithm specifications," Tech. Rep., May 1998. [Online].Available: http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf
[15] K. Singh and V. Muthukkumarasamy, "Authenticated key establishment protocols for a home health care system," in Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on, dec. 2007, pp. 353–358.
[16] S. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," in Research in Security and Privacy, 1992. Proceedings. 1992 IEEE Computer Society Symposium on, May 1992, pp. 72 –84.
[17] B. Tong, S. Panchapakesan, and W. Zhang, "A three-tier framework for intruder information sharing in sensor networks," in Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON '08. 5th Annual IEEE Communications Society Conference on, June 2008, pp. 451 –459. 100
[18] M. Kim and K. Chae, "Adaptive authentication mechanism using node reputation on mobile medical sensor networks," in Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on, vol. 1, Feb. 2008, pp. 499 – 503.
[19] K. Malasri and L.Wang, "Addressing security in medical sensor networks," in Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments, ser. Health Net '07. New York, NY, USA: ACM, 2007, pp. 7–12. [Online]. Available: http://doi.acm.org/10.1145/1248054.1248058
[20] K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 6, no. 11, pp. 4136 –4144, November 2007
[21] X. Du, S. Guizani, Y. Xiao, and H.-H. Chen, "Nis01-1: An efficient key management scheme for heterogeneous sensor networks," in Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE, 27 2006-dec. 1 2006, pp. 1 –5
[22] S. Camtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," Networking, IEEE/ACM Transactions on, vol. 15, no. 2, pp. 346 –358, April 2007.
[23] O. Morchon and H. Baldus, "Efficient distributed security for wireless medical sensor networks," in Intelligent Sensors, Sensor Networks and Information Processing, 2008. ISSNIP 2008. International Conference on, dec. 2008, pp. 249 – 254.
[24] R. L. Rivest, "The rc5 encryption algorithm," in Fast Software Encryption, 1994, pp. 86 –96.
[25] D. E. Eastlake and P. E. Jones, "US secure hash algorithm 1 (SHA1)," Tech. Rep. [Online]. Available: http://www.ietf.org/rfc/rfc3174.txt?number=3174
[26] NIST Special Publication 800-38A, [Online]. Available:http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
[27] Digital cellular telecommunications system (Phase 2+), "Security mechanisms for SIM application toolkit; Stage2", (3GPP TS 03.48 version 8.8.0 Release 1999). 101
[28] Eric Southern, Abdelkader Ouda and Abdallah Shami, "Wireless Security: Securing Mobile UMTS Communications from interoperation of GSM", submitted to Special Issue on "Security in Wireless Ad Hoc and Sensor Networks with Advanced Q Provisioning",Wiley Journal on Security and Communication Networks.
[29] "Brief History of GSM & the GSMA", GSM Association. 2008; http://www.gsma.com/aboutus/history/ (19 June 2012).
[30] GSM 02.09, "Digital cellular telecommunications system (Phase 2+); Security Aspects", version 6.1.0, Release 1997.
[31] A Kerckhoff, "La cryptographie militaire," Journal des sciences militaries, vol. IX, p. 538, Jan 1883.
[32] A. Biryukov, A. Shamir, and D.Wagner, "Real time cryptanalysis of a5/1 on a pc," in In FSE: Fast Software Encryption. Springer-Verlag, 2000, pp. 1-18..
[33] E.Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of gsm encrypted communication." Springer-Verlag, 2003, pp. 600-616.
[34] 3GPP,"Secuirty Objectives and Principles," https://www.3gpp.org/ftp/Specs/htmlinfo/ 33120.htm, 3rd Generation Partnership Project (3GPP), TS 33.120, (Apr. 2001).

[35] O. Dunkelman, N.Keller, and A. Shamir, "A practical-time attack on the a5/3 cryptosystem used in third generation gsm telephony," Cryptology ePrint Archive, Report 2010/013, 2010.
[36] G. Mapp, M. Aiash, A. Lasbae, and R. Phan, "Security models for heterogeneous networking," in Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, July 2010, pp.1-4.
[37] Scott Fluhrer, Itsik Mantin, and Adi Shamir. "Weaknesses in the key scheduling algorithm of RC4", Lecture Notes in Computer Science, 2259:1–24, 2001.
[38] GPP TS 33.102, "3G Security; Security architecture", Release 9, 2009.
[39] 3GPP TS 33.401, "3G security; Security architecture, 3GPP System Architecture Evolution (SAE); Security architecture", Release 11, 2011.
[40] M. Burrows, M. Abadi, R. Needham. "A logic for authentication," DEC System Research Technical Report No 39, Feb 1989. 102
[41] 3GPP TR 33.902, "Formal analysis of 3G authentication and key agreement protocol", V4.0.0, 2001-09.
[42] Shi Shi-ying; Mao Yu-ming; , "An Improvement Key Distribution Protocol and Its BAN Analysis," Future Computer and Communication, 2009. ICFCC 2009. International Conference on , vol., no., pp.381-384, 3-5 April 2009
[43] Cai Qingling; Zhan Yiju; Wang Yonghua; , "A Minimalist Mutual Authentication Protocol for RFID System & BAN Logic Analysis," Computing, Communication, Control, and Management, 2008. CCCM '08. ISECS International Colloquium on , vol.2, no., pp.449-453, 3-4 Aug. 2008
[44] Abdellatif, R.; Aslan, H.K.; Elramly, S.H.; , "New real time multicast authentication protocol," Computer Engineering & Systems, 2008. ICCES 2008. International Conference on , vol., no., pp.245-250, 25-27 Nov. 2008
[45] Maglogiannis, I.; Kazatzopoulos, L.; Delakouridis, K.; Hadjiefthymiades, S.; "Enabling Location Privacy and Medical Data Encryption in Patient Telemonitoring Systems," Information Technology in Biomedicine, IEEE Transactions on , vol.13, no.6, pp.946-954, Nov. 2009
[46] Al-Muhtadi, J.; Campbell, R.; Kapadia, A.; Mickunas, M.D.; Seung Yi; , "Routing through the mist: privacy preserving communication in ubiquitous computing environments," Distributed Computing Systems, 2002. Proceedings. 22nd International Conference on , vol., no., pp. 74- 83, 2002
[47] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The SecondGeneration Onion Router," in Proc. of the 13th USENIX Security Symposium, 2004.
[48] Garcia-Morchon, O.; Falck, T.; Heer, T.;Wehrle, K.; , "Security for pervasive medical sensor networks, "Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous, 2009. MobiQuitous '09. 6th Annual International , vol., no., pp.1-10, 13-16 July 2009
[49] Jinyuan Sun; Xiaoyan Zhu; Yuguang Fang; , "Preserving Privacy in Emergency Response Based on Wireless Body Sensor Networks," Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE , vol., no., pp.1-6, 6-10 Dec. 2010