ISSN 2347- 6893

Security of Wireless Sensor Networks in Biomedical

Muneer Alshowkan[1], Christian Bach[2], Ammar Odeh[3]

Abstract :–

Wireless sensor networks are rapidly growing as they have many outstanding characteristics such as the low power consumption, remote location sensing, low cost wirelessly communication and mobility. There has been increase in using wireless sensor networks in the biomedical and healthcare. However, using wireless sensor network introduce new challenges that are related to privacy and security. As well as the information related to the patient besides the other parities in the healthcare facilities. For instance, the information related to the doctors, nurses and the workers. We reviewed the latest approaches that are related to wireless sensor security in the literature and identified the most affective factors in wireless sensor networks that are affecting the privacy and the security when employing these network especially in biomedical field. We discuss the tradeoff between increasing the security and the network performance. Moreover, we provide several solution to increase the security of wireless sensor network while maintaining the required performance. - In this we have covered the security issues that are related to the computing network. However, the risk from using the devices in the human body are not the scope of this paper. The purposed solutions are more effective when taking in consideration the factors the effect the wireless sensors such as the battery life or providing new a valid source of power. This paper provide the challenges of using the wireless sensor network in biomedical field and how to solve most of these issues. Solutions are provided to be implemented with the consideration of the other factors provided to make the wireless sensor network more secure.

Keywords: Wireless Sensor; Biomedical Sensor; Biomedical Security; Patient; Privacy; Confidentiality.

Council for Innovative Research

Peer Review Research Publishing System

Journal: Journal of Advances in Biology

Vol. 2, No. 2

editor@cirworld.com

www.cirworld.com, member.cirworld.com

[1] University of Bridgeport, Bridgeport ,CT 06604

[2] University of Bridgeport, Bridgeport ,CT 06604

[3] University of Bridgeport, Bridgeport ,CT 06604

INTRODUCTION

Wireless sensor network (WSN) consist of many small in size devices, powered by batteries, have computing capabilities and distributed in an application area. The goal of these devices is to sense, measure and transfer the application data to the base station. There are many applications for the wireless sensor networks where the sensors are responsible to sense and collect some values of interest such as vibration, temperature, humidity, light, sound, electrocardiogram, pulses, and other related healthcare applications. The sensor are sending the information or data as light, sounds or text however, these messages are known to the wireless sensor application users [1]. There are many fields where the wireless sensor networks are active for instance; they are used for the environmental applications, industry applications, military applications and healthcare applications. Speaking about the applications, wireless sensor networks are deployed for monitoring the applications that are difficult to monitor using the conventional monitoring methods for example, geological application for monitoring in [2, 3] , smart space monitoring application in [4] ecological application in [5], education in [6] and aircraft application in [7]

The growth and the wide spread of the wireless sensor networks introduced a new types of applications for wireless sensor networks in our live. And as the human healthcare is the most valuable and rapidly growing field. The evolution for technologies to design devices that is able to aid in human healthcare. Such devices are small in size, wearable and can be integrated with the conventional devices. Moreover, the small sensors the patients use could for an on-demand infrastructureless network such s ad hoc network. As a result, the patients can continuously send their data to their healthcare providers as if they are carrying a PDA or portable computer [8, 9].

There are any benefits for using the wireless sensor network. These benefits are utilized for both the patient and the physician. For instant, the benefit for the patient could be by providing continuously monitoring for the patient health. However, the physician comes from the continuously and accurate data of the patient allow for more accurate diagnoses. Moreover, wireless sensor networks allow flexibility in treatment where the patient's data are sent while the patients are in their environment instead of using the fixed wired biomedical devices in the healthcare facilities.

Considering the medical devices can be divided into two groups. First, stand-alone devices which are intended to perform a specific monitoring for the application and actuation action however, this group doesn't need to interact with medical devices. This group is has the biggest share from the medical devices that are being used. Second the communication devices, which are different than the stand alone ones as they are able to interact with the surrounded devices using wireless communication. For instance, monitoring the patients in [10], pacemakers [11], the pulse oximeters [12].

Regarding to wireless sensor networks in biomedical field, the applications can be classified in several areas notably, monitoring the patients, the actuator and the biomedical systems. However, there are challenges that affect using the wireless sensor network in biomedical field such as the confidentiality, privacy, availability, physical security, limitation in resources and fault tolerance. Moreover, we should notice that many of the challenges are related to the wireless sensors networks however, the deployment on biomedical add more constrains and raise new issues [13].

In this paper we are identifying the key issues that are affecting deploying the wireless sensor networks in the biomedical field. These issues that are related to the patients' data confidentiality, data privacy and data availability

WSN APPLICATIONS IN BIOMEDICAL

Wireless sensor networks in healthcare are deployed outside or inside the patient body. Outside the body which is involves placing the sensors around the body. At the other hand, inside the body involves implanting the wireless sensor network inside the patient body. When placing several sensors in or outside the body they form a network called BAN (body area network) or PAN (personal area network). The collected data can be sent to a cluster head device for aggregation or passed to another node to be forwarded to the base station. Dependent on the application the wireless sensors network functions and operations will be determined [14]. For instance, data collection, aggregation, processing, forwarding, and analyzing [13].

RESEARCH METHOD

In recent literature many topics related to wireless sensor networks in biomedical applications exist. After reading over fifty articles in the recent literature that are related to wireless sensor networks security in biomedical field, we identify the key studies here. Moreover we identify the key challenges that required to be studied to achieve the ultimate goal which is to secure the wireless sensor networks in biomedical field.

One of the applications is related to physiologic monitoring by sensing the patients related data. The data collected can be forwarded to clinicians, researchers, physicians, and other health care providers to be used for present or future reference. Collected data is utilized to alert healthcare providers on a moment's notice of any abnormalities [15]. Applications pay special attention to critical patient data such as monitoring blood pressure, pulse, oxygen, blood sugar, and electrocardiogram data [16-19].

In [20] they discussed the body action recognition by deploying several sensors on the body to detect sounds and movements which later can be analyzed. In another publication by Jovanov at el. studied the use of personal locators which can analyze the relationship between stress and their subjects environment [21]. For patients with serious conditions such as diabetes or hypoglycemia applications can continuously monitor their blood levels [18, 19, 21]. These applications proved to be more valuable than the average medical records as the data is constantly updated and analyzed in real time [22].

In other works patients habits based on their activities in their current environment was studied in [5, 8, 23-25]. Some systems are specially designed for specific needs for patients care such as medication monitoring [23]. Monitoring the recovery of stroke patients through the telecommunication channels known as e-rehabilitation [26].

Security Threats within WSN Applications in Biomedical

The security threads in networks can be classifies in to two categories: passive and active attacks fig 1. Passive attacks cover the attacks that are related to disclose the confidential information such as reading of secret messages and analyze the network traffic however; these attacks are done by eavesdropping and are not intended to change the data.

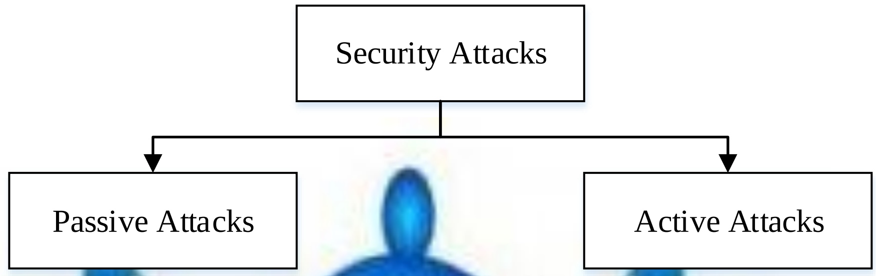

Figure 1 Passive and Active Attacks

At the other hand the active attacks which are aiming to create, modify or interrupt the information for instance, message modification and denial of service. Considering these attacks, the attacker can violate the confidentially, integrity and the availability of patients and health providers data. Following this further, confidentially includes data confidentiality and privacy. The integrity includes the data, system integrity fig 2.

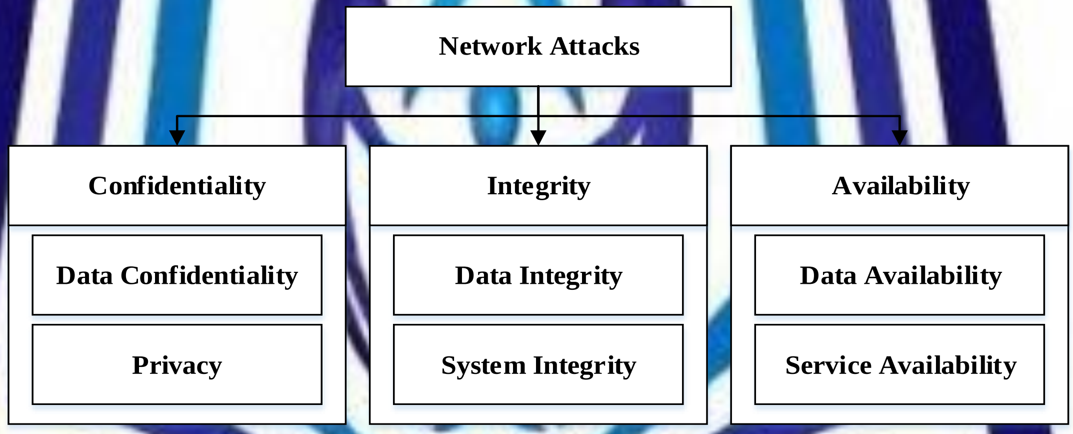

Figure 2 Attacks on Networks

Speaking about the security of wireless sensor networks in healthcare and biomedical field, there are four types of attacks related to attacks in networks. Three of them related to the patient and one is related to the healthcare provider for the patients, the physical security, data security and the physical security of the device for the healthcare provider, the data of the healthcare provider [27]. The physical security of the patient attacks includes the attacks the aim to harm the patient health directly. This type of attacks can be achieved using the function and services of the sensing devices which are the device communication, sensing, processing and communication. Data security mostly concerns itself with the protection of a patient's confidential health records. Patient health records not only contain identity information, but also sensitive information that could disturb a patient's personal relationships, job or career advancement opportunities. Physical attacks on the medical devices and networks from the attacks that aim to disturb the network and it's devices from their intended functions, such as the denial of service attacks. At the other hand the attacks on the healthcare provider data aiming to compromise the healthcare provider internal network and data.

PROPOSED MODEL

To provide the necessary protection for the wireless sensor network when we use it in the biomedical and healthcare field, we need to identify the network threads and require measurements. Many of the attacks are similar to the attacks in normal wireless sensor network but when these networks are used in the biomedical field new challenges are introduced. Moreover they type of the data in these networks when they are used in biomedical applications become sensitive as they are related to the patient health and compromise these data in critical. To protect these network there a need to address the related factors that are affecting the wireless sensor networks security which are the following in fig 4:

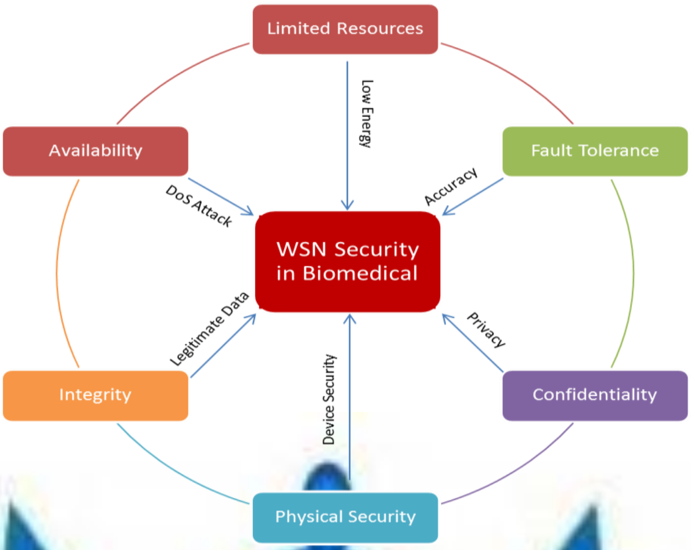

Figure 3 The Model to Secure WSN

Limited Resources

Wireless Sensors have limited energy and usually they operate using batteries. These batteries are required to be changed or recharged after a period of time. However, there are some of attacks that target the wireless sensor to exhaust the device so it lose its powers and die. There for, a protection is needed from some of the unauthorized connections that aim to exhaust the wireless sensor are required.

To solve the energy limitation in wireless sensor network many researchers have conducted studies. In fact the limited resources such as in energy have a great effect on the wireless sensor security. That because when adding security measures such as encryption extra processing and data transmission will be added as an overhead cost which will affect the sensor energy consumption and shortage it's functioning life. Moreover, a study in [28] aimed to find the best encryption algorithm that fits the wireless sensors networks in biomedical. Many algorithm were studied based on their performance and the energy consumption and concluded by finding MISTY1 encryption algorithm is the best to be used. Considering the routing protocol in wireless sensor networks and their ability to play a major role in reserving the sensor resource, protocols such is Hybrid Indirect Transmission [29] is designed to lower the resources when transmitting data. HIT is based on clustering and utilize data fusion. Moreover, HIT has different mechanisms such as Carrier Sense Medium Access with Collision Detection where the sender after finding the medium is free sends the data and listen in the medium in case of collision happen. HIT also use Time Division Multiple access where each sensor can occupy the whole medium for certain amount of time. Finally, HIT uses mechanism from LEACH protocol (Low Energy Adaptive Clustering Hierarchy) [30]. Overcoming the resources limitation in wireless sensors network is essential when implementing security measures are required to reduce the effect of the security overhead costs.

Fault Tolerance

Because of the nature of the data the wireless sensor is sending, it's important to make sure that the data is accurate as the healthcare provider depend of these data to diagnose the patient. However, faults in wireless sensors are provoked by the lack of energy or during the transmission. In fact, the failure could be in some of the transmitted data or in all the data. Other causes of failure could data congestion in the network and an attack on the data during transmission. In [25] a study have been done to identify the threats related to fault tolerance and interferences. As a result, the authors indicated that these issues are still open in wireless sensors network and there is no protocol currently solving them. Speaking about interference and jamming, FHSS (frequency hopping spread spectrum) and DSSS (Direct sequence spread spectrum) are traditional solutions. However, there are cost of implementing these techniques in term of power consumption. A study to was conducted to address routing issues, power consumption, where a signal jamming and node faults using a signal with priority properties to detect the jamming location was proposed in [31]. Further, detecting the interference in Body Area Network using a coordinator was proposed in [32] where this coordinator checks for the existing of the interfering packets. A role based system was proposed to overcome different types of security issues related to wireless sensor network [33]. Where the system after detecting the compromised node, it stops from having to function in the network. Another technique that uses different process aiming to mitigate the effect of the compromised node was proposed in [34]. In [35] a solution was proposed based on having communication with neighbors to avoid having a communication failure in the network in case of an attack on the network. As the neighbor nodes store the packets it they listen and track the connection until it fully received by the destination node.

Confidentiality, Integrity and Availability

To protect the patient data a security mechanism is required. Using authentication and encryption are required to assure the patient data security and privacy. Considering aggregation data from different nodes in the network before having the data to be processed and sent to the sink, data confidentiality, fault tolerance and robustness are required [36]. In fact, wireless sensor applications for biomedical must have the necessary encryption and authentication service to guarantee the confidentially and the privacy of the patients and the healthcare facility. That is, confidentiality is required to protect the patient's data and authentication to assure the legitimacy of nodes in the network avoiding an attacker to join the network and place attacks that lead to denial of service (DoS). Another encryption scheme was proposed in [37] which an identity-based for body sensor network. In [16] The authors have proposed a model for body are network to provide the require authentication. As the signal was design to be transmitted through multi-hop within the nodes in the body.

Key distribution is wireless sensor network is one of the challenges when trying to employ encryption and authentication services. Therefore, pre-distributed keys is adopted to reserve the network energy. Moreover, many of security services that require keys are using the pre-distributed keys scheme [38, 39]. As having the sensors to be deployed we pre-distributed and shared key can solve the problem of key distribution after deploying the sensors. Moreover, change the keys using the permanent key is essential or avoid having the key to be intercepted and known by an attacker. As a result, this will prevent the attacker for decrypting the messages and join the network to perform denial for service attacks threating the availability of the network. Considering the routing protocol LEACH [30] which is an energy efficient routing protocol based on clustering. Where many protocol tried to improve it by adding security services. For instance, having pre-distributed keys for symmetric encryption, involving secure broadcast authentication such as µTESLA [40]. Further, public key cryptography was also purposed with the implementation of ECC to reduce the energy consumption as in [40, 41]. Implementing the required security service in wireless sensors network to protect the BAN require having lightweight protocols the preserve the energy. For example, having a sensor inside the patient body need to have an energy source that doesn't make it necessary to have the patient to have to perform an operation to recharge the battery to change the sensor.

Physical Security

The hard ware device itself need to be protect from unauthorized access where and attack could be able to access the patient information from the physical device. Another concern is about the ability of the sensor to function inside the patient body or under the skin [42]. Moreover, the sensor components and materials must be made from materials that is not harmful of the body and the body should be able to accept it inside. As these factors might provide greater risk to the patient from the benefits that reflect the use of wireless sensor networks inside the body.

Proposed Model Discussion

This model discusses they key factors that affect the wireless sensor network in biomedical field. As providing the necessary measurements for each factor is essential to have the required security that is needed in the biomedical and healthcare field [13]. An encryption for the data is essential but it need to combine with low energy routing protocols and over all low energy consumption network.

Importance of the Model

Considering the security issues the wireless sensors networks are facing. The model covers all the essential keys that are need to protect the network from different types of attack. Employing the encryption to assure the confidentiality and the privacy and authentication to provide the availability of the network which are the key to make wireless sensor network secure and mitigate the attack that target the network resources.

Conclusion

There are many benefits we can we can utilize using the new technologies however, it always introduce new challenges. Wireless sensor networks biomedical in new emerging technology but has some challenges that need to be addressed. In this paper we have provided a solution to one of these challenges where the wireless sensor network needs to be secured to provide protection for the patient and the healthcare provider. Where the data must be encrypted and transmitted using low energy network. As a result, that will make the patient assuring the confidentiality, privacy and prolong the need to maintain the wireless sensor itself.

References

[1]T. J. Dishongh, M. McGrath, and B. Kuris, Wireless sensor networks for healthcare applications: Artech House, 2009.

[2]G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, et al., "Deploying a wireless sensor network on an active volcano," Internet Computing, IEEE, vol. 10, pp. 18-25, 2006.

[3]G. Werner-Allen, J. Johnson, M. Ruiz, J. Lees, and M. Welsh, "Monitoring volcanic eruptions with a wireless sensor network," in Proceeedings of the Second European Workshop on Wireless Sensor Networks, 2005, pp. 108-120.

[4]K. Mills, J. Scholtz, and K. Sollins, "Special Issue on Smart Spaces and Environments," IEEE Personal Communications, vol. 7, pp. 35-42, 2000.

[5]A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, 2002, pp. 88-97.

[6]M. Srivastava, R. Muntz, and M. Potkonjak, "Smart kindergarten: sensor-based wireless networks for smart developmental problem-solving environments," in Proceedings of the 7th annual international conference on Mobile computing and networking, 2001, pp. 132-138.

[7]B. Haowei, M. Atiquzzaman, and D. Lilja, "Wireless sensor network for aircraft health monitoring," in First International Conference on Broadband Networks, 2004, pp. 748-750.

[8]T. Dimitriou and K. Ioannis, "Security issues in biomedical wireless sensor networks," in Applied Sciences on Biomedical and Communication Technologies, 2008. ISABEL '08. First International Symposium on, 2008, pp. 1-5.

[9]V. Shnayder, B.-r. Chen, K. Lorincz, T. R. F. Jones, and M. Welsh, "Sensor networks for medical care," in Conference On Embedded Networked Sensor Systems: Proceedings of the 3 rd international conference on Embedded networked sensor systems, 2005, pp. 314-325.

[10]B. Vijayalakshmi and C. Ram Kumar, "Patient monitoring system using Wireless Sensor based Mesh Network," in Third International Conference on Computing Communication & Networking Technologies (ICCCNT), 2012, pp. 1-6.

[11]H. Huang, P.-Y. Chen, M. Ferrari, Y. Hu, and D. Akinwande, "Dual band electrically small non-uniform pitch ellipsoidal helix antenna for cardiac pacemakers," in Radio and Wireless Symposium (RWS), 2013 IEEE, 2013, pp. 325-327.

[12]K. Li, S. Warren, and B. Natarajan, "Onboard Tagging for Real-Time Quality Assessment of Photoplethysmograms Acquired by a Wireless Reflectance Pulse Oximeter," Biomedical Circuits and Systems, IEEE Transactions on, vol. 6, pp. 54-63, 2012.

[13]E. Stuart, M. Moh, and M. Teng-Sheng, "Privacy and security in biomedical applications of wireless sensor networks," in First International Symposium on Applied Sciences on Biomedical and Communication Technologies, 2008, pp. 1-5.

[14]S. Misra, V. Tiwari, and M. S. Obaidat, "Lacas: learning automata-based congestion avoidance scheme for healthcare wireless sensor networks," Selected Areas in Communications, IEEE Journal on, vol. 27, pp. 466-479, 2009.

[15]M. Gaynor, S. L. Moulton, M. Welsh, E. LaCombe, A. Rowan, and J. Wynne, "Integrating wireless sensor networks with the grid," Internet Computing, IEEE, vol. 8, pp. 32-39, 2004.

[16]T. Falck, H. Baldus, J. Espina, and K. Klabunde, "Plug'n play simplicity for wireless medical body sensors," Mobile Networks and Applications, vol. 12, pp. 143-153, 2007.

[17]J. Riudavets, K. F. Navarro, E. Lawrence, R. Steele, and M. Messina, "Multi router traffic grapher(MRTG) for body area network(BAN) surveillance," WSEAS Transactions on Computers, vol. 3, pp. 1856-1862, 2004.

[18]W. H. Baumann, M. Lehmann, A. Schwinde, R. Ehret, M. Brischwein, and B. Wolf, "Microelectronic sensor system for microphysiological application on living cells," Sensors and Actuators B: Chemical, vol. 55, pp. 77-89, 1999.

[19]L. Schwiebert, S. K. Gupta, and J. Weinmann, "Research challenges in wireless networks of biomedical sensors," in Proceedings of the 7th annual international conference on Mobile computing and networking, 2001, pp. 151-165.

[20]J. A. Ward, P. Lukowicz, G. Troster, and T. E. Starner, "Activity Recognition of Assembly Tasks Using Body-Worn Microphones and Accelerometers," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 28, pp. 1553-1567, 2006.

[21]E. Jovanov, A. O"Donnell Lords, D. Raskovic, P. G. Cox, R. Adhami, and F. Andrasik, "Stress monitoring using a distributed wireless intelligent sensor system," Engineering in Medicine and Biology Magazine, IEEE, vol. 22, pp. 49-55, 2003.

[22]M. Wang, M. Blount, J. Davis, A. Misra, and D. Sow, "A time-and-value centric provenance model and architecture for medical event streams," in Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments, 2007, pp. 95-100.

[23]L. Ho, M. Moh, Z. Walker, T. Hamada, and C.-F. Su, "A prototype on RFID and sensor networks for elder healthcare: progress report," in Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis, 2005, pp. 70-75.

[24]P. Kulkarni and Y. Öztürk, "Requirements and design spaces of mobile medical care," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 11, pp. 12-30, 2007.

[25]L. Paradis and Q. Han, "A survey of fault management in wireless sensor networks," Journal of Network and Systems Management, vol. 15, pp. 171-190, 2007.

[26]H. Zheng, N. D. Black, and N. D. Harris, "Position-sensing technologies for movement analysis in stroke rehabilitation," Medical and biological engineering and computing, vol. 43, pp. 413-420, 2005.

[27]D. Arney, K. K. Venkatasubramanian, O. Sokolsky, and L. Insup, "Biomedical devices and systems security," in Engineering in Medicine and Biology Society,EMBC, 2011 Annual International Conference of the IEEE, 2011, pp. 2376-2379.

[28]C. Strydis, D. Zhu, and G. N. Gaydadjiev, "Profiling of symmetric-encryption algorithms for a novel biomedical-implant architecture," in Proceedings of the 5th conference on Computing frontiers, 2008, pp. 231-240.

[29]B. J. Culpepper, L. Dung, and M. Moh, "Design and analysis of Hybrid Indirect Transmissions (HIT) for data gathering in wireless micro sensor networks," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 8, pp. 61-83, 2004.

[30]W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on, 2000, pp. 1-10.

[31]N. Ahmed, S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: a survey," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 9, pp. 4-18, 2005.

[32]R. C. Shah and L. Nachman, "Interference detection and mitigation in IEEE 802.15. 4 networks," in Proceedings of the 7th international conference on Information processing in sensor networks, 2008, pp. 553-554.

[33]B. Panja, S. K. Madria, and B. Bhargava, "A role-based access in a hierarchical sensor network architecture to provide multilevel security," Computer Communications, vol. 31, pp. 793-806, 2008.

[34]M.-Y. Hsieh, Y.-M. Huang, and H.-C. Chao, "Adaptive security design with malicious node detection in cluster-based sensor networks," Computer Communications, vol. 30, pp. 2385-2400, 2007.

[35]S.-B. Lee and Y.-H. Choi, "A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks," in Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, 2006, pp. 59-70.

[36]R. C. Luo, Y. Chih-Chen, and S. Kuo-Lan, "Multisensor fusion and integration: approaches, applications, and future research directions," Sensors Journal, IEEE, vol. 2, pp. 107-119, 2002.

[37]C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: an identity-based cryptography approach," in Proceedings of the first ACM conference on Wireless network security, 2008, pp. 148-153.

[38]F. Hu, W. Siddiqui, and K. Sankar, "Scalable security in Wireless Sensor and Actuator Networks (WSANs): Integration re-keying with routing," Computer Networks, vol. 51, pp. 285-308, 2007.

[39]K. M. Martin and M. Paterson, "An application-oriented framework for wireless sensor network key establishment," Electronic Notes in Theoretical Computer Science, vol. 192, pp. 31-41, 2008.

[40]A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Wireless networks, vol. 8, pp. 521-534, 2002.

[41]B. Doyle, S. Bell, A. F. Smeaton, K. Mccusker, and N. E. O'Connor, "Security considerations and key negotiation techniques for power constrained sensor networks," The Computer Journal, vol. 49, pp. 443-453, 2006.

[42]T. Daisuke, X. Yang, H. Fei, C. Jiming, and S. Youxian, "Temperature-aware routing for telemedicine applications in embedded biomedical sensor networks," EURASIP Journal on Wireless Communications and Networking, vol. 2008, 2008.