ISSN 2320 - 2602
Volume 5 No.8, August 2016
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst02582016.pdf

A Review of Network Security Methods in Cybercrime for Wireless Body Area Networks Care

I.Shanmugapriya[1] Dr. K.Karthikeyan[2]
PhD Scholar, Assistant Professor, Dr.SNS Rajalakshmi College of Arts and Science (Autonomous), Coimbatore – 49, Email Id:sachiinsharan@gmail.com
Head Department of Computer Science, Government Arts and Science College, Karambakudi, Pudhukottai (Dt) TamilNadu, India, Email id: ithodsns@gmail.com

ABSTRACT: Wireless Body Area Networks (WBANs) have been become a more interesting and investigation study in recent years, because they provides many services for remote health monitoring and real-time applications specifically for patient care. On the other hand by using any type of wireless communication medium, information security in WBANs is a difficult task and major issue in the recent years. Because WBANs includes of small sensors placed on the human body, they require resource and computational limitations, thus building the use of difficult and advanced encryption algorithms infeasible. This motivates the creation of new security protocol/ algorithm which requires less resource and less computational complexity thus achieves high security in WBANs. This paper presents a review of the security schemas suitable for WBANs that are independent to each other and new key management for enhancing the security of WBANs. In this paper review the survey regarding cybercrime on WBANs and some methodology used in the literature for preventing those cybercrime is also discussed simultaneously. This survey majorly study the details of network security and those results were compared to two methods that is Genetic algorithm (GA) and GA combined with Cox regression (CoRGA) .These methods is used for identifying a potential threat for Bodycare system and perform multi-hop routing algorithm using hierarchical protocols for safety transmission and finally some solution was inferred. The survey reviews the details of existing network security schemas with their own pros and cons. At finally the simplicity of the two security schemas CoRGA and GA provides high security. The proposed algorithms are validated by performance analysis.

Keywords: Body Area Networks (BAN), Security, cybercrime, schemas, Genetic Algorithm (GA), Cox regression (CoR), Wireless Body Area Network (WBAN).

1.INTRODUCTION

Human health monitoring have been becomes one of the most important investigative research area from the recent development in wireless communication and sensor technologies, which have allow the make use of sensors to support in recording biometric data vaguely. Sedentary lifestyles have been becomes one of the most increased the risks of potentially critical medical conditions such as high blood pressure, cardiac diseases, diabetes, and the like, at the same time as confused work schedules / deficiency of quality healthcare have give to rising their risks. Known their regular nature of degeneration of such conditions in a human being, regular and continuous monitoring presumes high priority.

So Body area networks (BANs) effortlessly connect a miniaturized and low-power device which consists of biosensors with the purpose of worn on or fixed in human body. The improvement of BANs is promising research, mainly to gather and together procedure biological data designed for continuous and long-term monitoring of health conditions [1–3]. Because medical and health data are private and sensitive information with the purpose of protected by means of law in several countries, for instance, by the Health Information and Portability Accountability Act (HIPAA) in the USA [4], the European Union Directive 2002/58/EC in Europe [5], and Law of the People's Republic of China on Medical Practitioners in China [6], the security of data transmission inside BANs should be addressed in order for them to be extensively second-hand in real-life health applications.

However BANs uses the common features of general Wireless Sensor Networks (WSNs), it is estimated with the purpose of the two networks must have extremely different security schemes. This type of the network is known as the Wireless Body Area Networks (WBANs) [7] are a type of wireless sensor networks, where a group of sensors are positioned or fixed in human body to measure the physiological parameters of a person and transmit it to the monitoring medical center or hospital. This have been performed via the use of Internet or a cellular network, they use a personal digital assistants (PDAs) as intermediary devices. However to achieve security in any network becomes critical. This, coupled with the fact that medical decisions are made based on the data received, assumes significant focus in the research on WBANs.

To achieve security in WBANs, the messages have been transmitted from source to destination by encrypting original message using encryption schemes with key and decrypted at the destination or receiver end. Several encryption algorithms have been proposed in the literature which are used for securing WBANs, on the other hand these methods have not obtain the general problems such as power constraints and resource constraints since they are small sensor devices residing on a person [8]. Thus, it becomes crucial to design algorithms that are simple in computation and resource utilization, yet achieve the desired security. At the heart of any encryption algorithm is the successful management of the special encryption key. The key generation scheme must also be computationally inexpensive yet secure.

In short, security methods designed for WBANs must not be straightforwardly assumed from conventional approaches. In this paper, we survey to summarize the details of the existing and conventional approaches used for implementing security approaches for BANs. The remaining section of the survey is summarized as follows. In section 2 presents the details of IEEE standard 802.15 communication protocols for WBANs. Then discussed the security methods used for IEEE standard 802.15 communication protocols in Section 3. Public Key Cryptography (PKC) and Symmetric Key Encryption (SKE) etc., for BANs and WBANs are, respectively, summarized in Section 4. Some common security Threats occurs in BANs and WBANs is discussed in Section 5. Finally, conclusions are drawn in Section 6.

2.COMMUNICATION PROTOCOLS USED FOR BAN AND WBAN

The regularity activity of WBANs is strongly succeeding approximately via the use of IEEE 802.15.6 TG BAN. Particular some system relying on target applications have proposed in the procedure and some of them have shown the possibility absolutely. The general architecture of system architecture of WBANs based on conventional methods is illustrated in Figure 1, which places major importance on a secure communication during data transmission stage. Figure 1 includes of group of application data servers (*m*), a central server to protect security against server, and multiple WBANs (*n*). A group of application data servers frequently categorized into two types such as medical or non-medical type. They have been proposed under wired or wireless networks with adequate resources designed for the difficult computational tasks such as encryption, decryption, and information processing. The central security server is dependable designed for key management process such as encryption, decryption, key management, key reuse, key revoking, renewing etc. One WBAN consists of group of wearable devices on the human body, a group of implantable devices such as biosensors or actuators fixed in the human body and a base station.

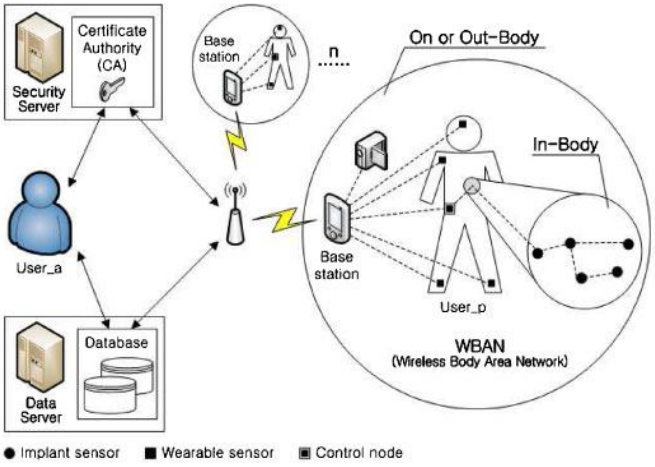

Figure 1. The system architecture of WBANs

The base station is dependable designed for gathering information of physiological signal features from determining components in WBAN and relaying the information to external application information or data servers as an alternative of each determining component, since they should have enough power toward transmit information in a long distance. It moreover has toward continues monitoring all conditions of each component in WBAN via wireless network. In common, we are able to infer with the purpose of a base station turn into an existing handheld device by means of moderately more power and computing resources in WBAN components and its functions are characterized via the use of plug-in software rather than separate specific hardware devices. These constraints of the base station confirm that it is the most significant part in terms of WBAN security. Thus in this research work, WBAN security is performed based on the focusing on a base station.

Each user has positively one or more control nodes connected to his or her body toward communicate by means of implantable biosensors. These types of nodes are fixed to human body, and those nodes are connected to a base station. They are responsible for gathering information of physiological signal features from determining components in WBAN and relaying the information to external application information. Because biosensors, mightn't have enough power toward transmit in the secret information to human body environment. Furthermore they are not possible to transmit information after a battery is restarted, consequently that they require to be monitored by periods. Physically, it is sufficient potential for the base station toward connect by means of all biosensors straightforwardly not including the control node. On the other hand, this system architecture of WBANs is not only sufficient in terms of energy itself , in addition it also handles human body strong and lasting a radio wave. The control node is able to moreover defend starting an attacker as a resulting firewall, and continue data in the short term when the base station is powered down in several reasons.

A biosensor comprises of set of processor, memory, transceiver, sensors/actuators, and a power unit. It performs some major steps such as sensing or processing information to the human body, transmitting it toward the control node toward trigger action inside the body. It is popular if communication be able to be avoided next to the expense of more computation and sensing. Consequently it is assumed with the purpose of not each and every one sensor in WBANs will be able toward communicate by means of the control node in a single hop however they do consequently by means of a multi-hop link all the way through other biosensors [9].

3. LITERATURE REVIEW OF SECURITY METHODS

Security in Wireless Body Area Networks (WBANs) is very challenging issues known with the purpose of the sensors transmit secret information regarding to the human body that continuously monitors the information of humans from base stations, and critical decisions are made based on this information. If the information being communicated was intercepted by means of an adversary, and altered, it should demonstrate critical to the patient. Security in Bodycare information systems is among the highest priority research areas as part of the new security framework for HIPAA compliant Bodycare information. This appraises security concerns in Bodycare information systems and concludes that what is needed is an approach that firmly cements the foundations for a sustainable and efficient Bodycare system based on solidarity and built to cope with the emerging threats. The model emerging from this approach would require a robust security infrastructure to support authentication, confidentiality, and data integrity so that there is no single point of failure that, if compromised, would give access to all the information. Consequently, this section of the review or survey some of the existing works related to the WBAN and BAN under network security.

3.1. METHODS FOR NETWORK SECURITY IN BAN

Tan et al [10] proposed a new Identity Based Encryption (IBE) cryptography approach to protect security in WBAN. They recognize the several security requirements in a WBAN, and present a new IBE scheme, named as IBE-Lite. In IBE, a random number is for public key generation, and secret key is generated to third party independently. On the other hand, every time a new public/secret key is generated independently, the secret key should be stored in the trusted Certificate Authority (CA), which poses several challenges the individual human to accesses the original data. In IBE-Lite, a sensor creates a public key by using random number; however, the sensors should not created secret keys. From this trusted third party might ensure security of information in WBAN.

Ali and Khan [11] developed a new broadcast-based key agreement scheme via the use of group of reconciliation designed secure data communication in WBANs. The proposed broadcast-based key agreement scheme permits the neighboring nodes toward agree upon a general key by means of the Personal Server (PS), created from the electrocardiogram (EKG) features subset of the host body. Smallest information is transmitted in a broadcast way, and even if the some nodes are missed from features subset, by merging these feature sets, the entire WBAN determination still agree upon an only one public key. Since they exchanges only limited information, if an attacker collects the information in any way, no one have a permission to reproduce the key. The proposed broadcast-based key agreement scheme alleviates replay, discriminating forwarding, and denial of service attacks by using a challenge-response authentication mechanism. The simulation results demonstrated that the proposed broadcast-based key agreement scheme produces best results in terms of the parameters like security, communication overhead, and running time complexity when compared to existing EKG-based key agreement scheme.

Some of the methods in the literature [12-13] are performed based on the pre-deployment which store some keys value in sensor memory earlier than performing the deployment phase. In [12] develop to make use of the adversary's uncertainty concerning the PHI transmission towards simultaneously update their personal key dynamically and enhance the security level. However the simulation results demonstrate that this proposed methods enhances security level under less usage of resource sensor platforms and less computational complexity.

Fuzzy Attribute-Based Signcryption (FABSC)[13] is proposed for key generation phase it make sure the safe distribution of private keys by means of choosing random polynomials. This method is performed under based on the some properties such as Received Signal Strength (RSS) and simulation characteristics of the WBAN. This proposed FABSC key generation schema is performed based on the procedure of fuzzy Attribute-based encryption towards facilitate data encryption, access control, and digital signature designed for a patient's medical data in a BAN. From the simulation results it concludes that the proposed FABSC key generation is proficient and feasible. But however this method suffers from forward secrecy problems, and also requires more memory usage, so these methods are unsuitable for WBANs.

In [14] the communicating sensors first sense the RSS values, and then apply the DWT for feature extraction. Novel key generation scheme is presented and a key distribution protocol, both of which are only based on wireless modules equipped on sensors. By exploiting the high correlation of Received Signal Strength Index (RSSI) between peer-to-peer communications, THIS scheme can provide a shared symmetric cryptographic key under the presence of an eavesdropper. The scheme in [15] involves

human interaction channel for secure key agreement process in WBAN.

3.2. CONVENTIONAL METHODS FOR NETWORK SECURITY IN BAN

Biometrics health care information system: In this paper different security issues will be explored which are associated with making the encrypted clinical messaging system secure. If a system is secure then this suggests that only authorized users can access it and the information that is being passed and stored within it. This new integrated system can link a plethora of patients to many GP[16-17] practices from different clinics, in Central London and can store very confidential information. The security of these patient records must be guaranteed. With this new system patients are able to receive their health records from the Internet. These systems also guarantee that sensitive information is staying private and cannot be intercepted from any other users except the individual patient.

Distributed Healthcare systems: The Distributed Healthcare systems [18] article summarizes and introduces into the basic security and reliability considerations for developing distributed software systems in Bodycare. It describes security objectives and protection of system assets. Stress is given to the need of risk analysis. Possible system vulnerabilities and system threats are enumerated. Necessary security awareness of humans, typical security and reliability requirements, as well as typical security methods and corresponding infrastructure for application protection, data protection and network protection are reflected.

Telemedicine and Teleradiology*:* Bodycare-information technology context as a backdrop for viewing legal issues that accompany telemedicine and teleradiology[19-20]. In this age of managed care, Bodycare informatics has become a burgeoning field. Computer-based technologies help automate processes such as patient data-collection. As patient records become increasingly digitized, they are more easily transmitted between various Bodycare sites and personnel. The security of electronic medical data transfer, however, is sometimes inadequate. Digitized medical records give rise to a number of legal issues. A well-known example is the security of electronic medical data. Data security and other legal issues pose enormous challenges to the adoption of Bodycare technologies; these barriers can potentially inhibit their diffusion. In the case of telemedicine, many of the current laws are underdeveloped and unstable, and pending bills are often obscure.

4. ISSUES FROM EXISTING WORK

For BANs and WBANs are designed for health applications, they should be protected from fraud nodes (1) eavesdrop health information (2) access health information without authorization (3) fabricate identity to verify authentication (4) deny health information with the purpose have been sent or received, and (5) alter health information. Based on these security threats under BANs and WBANs should include five major areas: confidentiality, authorization, authentication, nonrepudiation, and integrity control [21].

Confidentiality: To protect any personal health information from attacker, the authentic sensors might not exchange any information to inside the BAN and it can be performed by using incorporating encryption operations.

Authorization: To protect any personal health information of user's authorization should assign the access privileges and limit free access.

Authentication: To protect any personal health information of users includes entity authentication and data authentication. Entity authentication should verify the entities of the user during data exchange process. Data authentication permit a receiver toward confirm with the intention of the information really was sent by means of the claimed sender and protects an attacker or unauthorized user to report false health data of a BAN.

Nonrepudiation: Nonrepudiation guarantees with the purpose of an entity should not deny facts transmitted any message in BANs. Here some of the operations such as digital signature and digital certificate are able to provide nonrepudiation for the data transmission process of health information in BANs.

Integrity Control: Missing or wrong health information might result in critical outcomes to the owner of BANs. This can be verified by using integrity control step .It is completely essential where some modification of health information might be detected via the use of communication entities.

Several methods have been proposed in the literature based on the medical body sensor networks continuously. But these security methods become very difficult to provide high security and safety for medical BSN and WBSN. So Security Protocols for Sensors Networks (SPINS) is designed for obtaining some security requirements such as confidentiality, integrity and authenticity, and they uses a conventional cryptography methods. On the other hand, SPINS is only applied to conventional wireless sensor networks, so that it is inappropriate to apply in WBANs and BANs. Since WBANs consists of some additional environmental properties such as human body and limited computing resources.

On the contrary, some researches utilizing the asymmetric cryptosystem in mobile ad hoc networks also have been proposed [21], and tried to examine the unique characteristics of medical body sensor networks. One concern about the asymmetric cryptosystem is a resource

constrained problem, but recent work has shown that performing ECC public key computations on resource constrained devices is viable [22]. These researches dealt with a scope of limited WBANs that exclude the implanted sensor networks. The objective of WBANs is not only the solution of inconvenience but also the implementation of body area network that can contact with everywhere in, on, and out the human body. So, whether or not these technologies operate in ultra resource constrained bio-sensors of WBANs is yet to be known.

However all of the above mentioned biometric-based security schemes transmit entire feature subset to agree upon a common key. This makes less security during data communication of human personal data. So these methods are easily hacked by several attacks such as modification attack and forgery. Moreover, transferring the whole feature set increases the communication overhead, which reduces the performance and usability of the schemes.

5. PROPOSED METHODOLOGY AND RESULTS

In the past, this study explored the use of biological computational termed Genetic Algorithm (GAs)[22] combined with Cox regression (CoRGA)[23][24] in identifying a potential threat for Bodycare system. The results show that variable described "misused of e-mail" is the major information security threats for Bodycare system. Results were compared with manual analysis using the same data, and it is shows that Gas[23] not just introducing new threats for Bodycare system but it was similar with others threats proposed by previous researches. Here two methods were discussed one from protocols through Hierarchical Clustering and another one from genetic algorithm.

Table 1. Comparison of characteristics of the proposed protocols with other secure data transmission protocols

Metrics	**GA / CoRGA**	**Prior protocols**
key management	Asymmetric	Symmetric
Neighborhood authentication	Yes	Limited
Storage Cost	Comparative low	Comparative high
Network scalability	Comparative high	Comparative low
Communication overhead	Deterministic	Probabilistic
Computational Overhead	Low	Low to high
Attack	Passive and active attacks on wireless channel	

Genetic Algorithm: CoRGA[23] were used to analyze the best single risk, three and five factors contribute to security threats in Bodycare system. GAs was set to run with 100 generations and 50 genes in pool. Table 2 shows the descriptive characteristics of the variables selected by the GAs for three, four and five factors respectively. Columns 2 and 3 in Table I shows the variables selected by GAs for each size of chromosome and its generic vulnerabilities category and hazard ratios. It can be seen from Table I the single factor reported outdated software increased hazard ratio (HR 1.12). The second result shows that three factors did not really contribute to information security threats to Bodycare system i.e. (accidentally deletion or addition data by staff, misuse email by staff and failure to protect information by staff). GAs[26] selected five factors revelation accidently classified data by staff (HR = 1.29) and obsolete network equipment associated (HR 1.27) to the increasing of security problem into Bodycare system. Table 3 shows combination of 10 factors that contributed to security problems in Bodycare system. It can be seen from the results that four variables produced hazard ratio above 1.0 (i.e. server air conditioning failure, wireless network not secured, slow responses of server due to high consumptions of bandwidth and revelation accidentally classified by staff).

Table 2: Variables Selected by CORGA (Combination of one,three,five)

Variables	**Description**	**Hazard Ratios (HR)**
1	Outdated system software - Operating system	1.12
3	Accidental deletion or modification of data by staff	0.90
	Misuse of e-mail access by Staff	0.00
	Failure to protect information by staff	0.65
5	Slow response when viewing radiology images	0.75
	Introduction of damaging or disruptive software by staff	0.35
	Revelation accidently of classified data by staff	1.29
	Interruption by service provider – Electrical Department (TNB)	0.72
	Obsolete network equipment - Routers/Switches	1.27

Table 3. Variables Selected by CORGA (combination of 10)

Variable	Description	HR
10	System documentation is not systematically management	0.60
	Server air-conditioning failure due to power failure	1.34
	Slow response of server due to high consumptions of Bandwidth	1.80
	Slow response when viewing radiology images	0.57
	Interruption by service provider-Internet Service Provider(ISP)	0.66
	IP Spoofing attacks due to wireless network not secured	0.03
	Wireless network not secured	8.07
	Accidental deletion or modification of data by staff	0.56
	Revealation accidently of classified data by staff	1.82
	Outdated application staff	0.84

6. CONCLUSION AND FUTURE WORK

Human health monitoring have been becomes one of the most important investigative research area from the recent development in wireless communication and sensor technologies, which have allow the make use of sensors to support in recording biometric data vaguely. However to achieve security in any network becomes critical. This, coupled with the fact that medical decisions are made based on the data received, assumes significant focus in the research on WBANs. To achieve security in WBANs, the messages have been transmitted from source to destination by encrypting original message using encryption schemes with key and decrypted at the destination or receiver end. This paper review the details of several encryption algorithms have been proposed in the literature which are used for securing WBANs, on the other hand these methods have not obtain the general problems such as power constraints and resource constraints since they are small sensor devices residing on a person, So comparatively Genetic Algorithm (GA) is better than the other security encryption algorithms to protect bodycare details. However none of methods in the survey explore the effect of outdated software in information security risks which is considered as one of the further research. However in the future work ,the proposed schema is optimized to make use in various WBAN applications like medical and non-medical that must assure their technical properties while keeping implementation under the standardization of IEEE 802.15.6.

REFERENCES

1. Istepanian R.S.H, Jovanov E, and Zhang Y.T, "Introduction to the special section on m-health: beyond seamless mobility and global wireless health-care connectivity," IEEE Transactions on Information Technology in Biomedicine, vol. 8, no. 4, pp. 405–414, 2004.
2. Yuce M.R, Ng S.W, N. Myo N.L, Khan J.Y, and Liu W, "Wireless body sensor network using medical implant band," Journal of Medical Systems, vol. 31, no. 6, pp. 467–474, 2007.
3. Poon C and Zhang Y.T, "Perspectives on high technologies for low-cost healthcare," IEEE Engineering in Medicine and Biology Magazine, vol. 27, no. 5, pp. 42–47, 2008.
4. Hash J, Bowen P, Johnson A, Smith C.D, and Steinberg D.I, "An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule," National Institute of Standards and Technology, pp. 800–866, 2005.
5. Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002.
6. "Law of the people's Republic of China on medical practitioners," 1996, http://www.moh. gov.cn / publicfiles/business/ htmlfiles/mohzcfgs /s3576 /200804 / 18250.html.
7. Jafari R, Encarnacao A, Zahoory A, Dabiri F, Noshadi H, Sarrafzadeh M. Wireless sensor networks for health monitoring. Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05).
8. Malasri K, Wang L. SNAP: the architecture for secure medical sensor networks. 2nd IEEE Workshop on Wireless Mesh Networks, WiMesh 2006, 2006.
9. Singelee D, Latre B, Braem B, et al.Asecure cross-layer protocol for multi-hop wireless body area networks. ADHOC-NOW2008, LNCS 5198 2008; 94--107.
10. Tan CC,Wang H, Zhong S, Li Q. Body Sensor Network Security: An Identity-Based Cryptography Approach, Alexandria: VA, USA. 2008 (WiSec'08)
11. Ali, A., & Khan, F. A. (2014). A broadcast-based key agreement scheme using set reconciliation for wireless body area networks. Journal of medical systems, 38(5), 1-12.
12. He, D., Chen, C., Chan, S., Bu, J., and Zhang, P., Secure and lightweight network admission and transmission protocol for body sensor networks. IEEE J. Biomed. Health Inform. 17(3):664–674, 2013.

13. Hu, C., Zhang, N., Li, H., Cheng, X., and Liao, X., Body area network security: a fuzzy attribute-based signcryption scheme. IEEE J. Sel. Areas Commun. 31(9):37–46, 2013.
14. Wu, Y., Sun, Y., Zhan, L., and Ji, Y., "Low mismatch key agreement based on wavelet-transform trend and fuzzy vault in body area network". Int. J. Distrib. Sens. Netw. 2013:1–16, 2013.
15. Xin, H., Bangdao, C., Markham, A., Qinghua, W., Zheng, Y., and Roscoe, A. W., "Human interactive secure key and identity exchange protocols in body sensor networks". IET Inf. Secur. 7(1):30–38, 2013.
16. Gleni, S., Maple, C., & Yue, Y. (2009, April). "Security issues of a biometrics health care information system: the case of the NHS". International Conference on Computing, Engineering and Information, 2009(ICC'09), pp. 279-284.
17. Matousek, K. (2008). "Security and reliability considerations for distributed healthcare systems". In 2008 42nd Annual IEEE International Carnahan Conference on Security Technology ,pp. 346-348.
18. M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," IEEE Wireless Communications, vol. 17, no. 1, pp. 80–88, 2010.
19. A. Wheeler, "Commercial applications of wireless sensor networks using ZigBee," IEEE Communications Magazine, vol. 45, no. 4, pp. 70–77, 2007.
20. J. Szczepanski, E. Wajnryb, J. M. Amigo, M. V. Sanchez-Vives, and M. Slater, "Biometric random number generators," Computers and Security, vol. 23, no. 1, pp. 77–84, 2004.
21. Poon CCY, Zhang Y-T. "A Novel Biometrics Method to secure Wireless Body Area Sensor Networks for Telemedicine and M-Health". IEEE Communications Magazine 2006; 44(4): 73–81.
22. Malasri K, Wang L. "Design and implementation of a secure wireless mote-based medical sensor networks". UbiComp'08 Seoul, Korea, 21--24 September 2008
23. Rabiah Ahmad, Ganthan Narayana Samy, Nuzulha Khilwani Ibrahim, "Threats Identification in Healthcare Information Systems using Genetic Algorithm and Cox Regression".
24. Ahmad, R., Samy, G. N., Ibrahim, N. K., Bath, P. A., & Ismail, Z. (2009)." Threats identification in healthcare information systems using genetic algorithm and cox regression". Fifth International Conference on Information Assurance and Security, 2009. IAS'09. , Vol. 2, pp. 757-760.
25. Ahmad R and Bath PA, "The use of Cox regression and genetic algorithm (CoRGA) for identifying risk factors for mortality in older people", Health Informatics Journal Vol. 10 (3), 2004. pp. 221-236.