BioGecko

Vol 12 Issue 02 2023

ISSN NO: 2230-5807

COMPARATIVE STUDY OF CYBER SECURITY IN MEDICAL DOMAIN

Dhanashri S. Kulkarni
Research Scholar (JJTU) & Assistant Professor,Computer Science Department, Indira College of Commerce and Science, Pune Maharashtra, India.

Dr.Janardan A. Pawar
Associate Professor, Computer Science Department, Indira College of Commerce and Science, Pune Maharashtra, India.

Jyoti D. Shendage
Research Scholar(MGMU) & Assistant Professor,Computer Science Department, Indira College of Commerce and Science, Pune Maharashtra, India.

Abstract
The term "Cyber Security" refers to the methodology of preventing and responding to assaults on computer systems, networks, and software. Accessing, modifying, or erasing sensitive information in concern areas, extorting money from users, disrupting routine business procedures, etc., are all examples of digital assaults. The health and medical industry offers several opportunities for cyber security. The concern of this research investigation is to focus the safe practices in defined sectors. It is very well required from second generation of computing and will be required in future until there is computer and data in the digital world. The studies in cyber security are highly applicable in education, military, banking and many more where there are digital platforms. Now a day's medical sectors are also doing digital documentation and communication. Protection for such documents is required at highest priority level. To overcome the challenges, numerous researchers have developed more than 130 methods for ensuring it. IT practitioner has developed more than 50 strategies for handling and solving this issue. In this investigation we have reviewed the more than 22 studied pertaining to cyber security attacks and to prevention methods. This study is highly applicable for medical sector.

Keywords: Cyber Security, Medical,Sensor,WSN

1. Introduction

The integration of the Internet of Things (IoT) with the wireless sensor network (WSN) improves all activities that significantly reduce the need for human intervention and guarantee a higher standard of living for people, including monitoring of healthcare facilities, precision agriculture, traffic monitoring, and other similar activities. This development is both feasible from a technological standpoint and essential from an economic perspective. These sensor nodes have a tiny footprint yet are able to detect and interpret data despite their size. In comparison to conventional sensors, wireless sensor networks provide substantial advancements in terms of their sensing capabilities as well as their communication capabilities. "Although many aspects of sensor networks have been studied extensively, the bulk of research efforts have concentrated on network protocols, energy efficiency, and distributed databases. However, until now, there have been hardly any accomplishments in safeguarding WSNs. When sensor networks are used in critical infrastructure like hospitals, airports,

military bases, etc., it is imperative that they be protected from unauthorised access. A network is useless if proper security measures are not in place to protect the integrity and privacy of the information being sent." There are several security needs, including availability, the authenticity of origin, authentication of data, and secrecy. Although different applications may demand varying degrees of security, there are still many security requirements.

Recently, researchers using a subcategory of WSN known as Wireless Body Area Network have shown a substantial amount of interest in Internet of Things (IoT)-enabled smart healthcare monitoring systems (WBAN). Each individual patient works as a WBAN node in an IoT-enabled WBAN, and they are also outfitted with body sensors, also known as wearable sensors. This is done in order to regularly check the patient's health. A large data bank is required to allow the continuous monitoring of human vital indicators. Patients are assured of receiving superior medical treatment when they have access, both in the hospital and at home, to integrated computer devices that are outfitted with internet connections. Privacy, sensor location, intrusiveness, safety, and data management are some of the most difficult challenges that wireless sensor networks (WSN) present in hospital settings. All WSN applications have a key need that the information that has been gathered is successfully sent to the destination with as little end-to-end delay as possible. "This is achieved by the incorporation of cooperative and network-coded communication into the current WSN. Denial of service (DoS) attacks, eavesdropping, Sybil attacks, physical node manipulation, radio jamming, and replay assaults are just some of the cyber-security dangers that must be mitigated with robust security solutions in order to safeguard the healthcare data in sensor networks (also known as man-in-the-middle attacks)." In this paper, we attempt to analyse the study solutions for the smart healthcare monitoring system to achieve the security and privacy provisions from the different kinds of cyber-security vulnerabilities. We design the algorithms for cyber threats detection and its mitigation at the network layer with higher accuracy, optimal QoS performance, and minimum computation efforts.

The rise of the Internet of Things (IoT) for the applications like smart healthcare systems leads to several challenges like security, privacy preservation, energy consumption, and information loss caused by single or cross-layer cyber threats. Identifying and mitigating such cyber threats are key requirements for IoT-enabled applications. In this chapter, we present the introductory terms of the proposed research that mainly focused on the security and privacy preservation from the cross-layer threats in the WSN-assisted IoT networks.

Since from last decade, the various applications approved through the advancement in Wireless Sensor Network (WSN) like primary observing, military reconnaissance, mechanical estimations, & in particular in medical care applications [1]-[4]. Many of the know-how biomedical sensors serve as wearable units that likewise enhance smart medical care testing & furthermore help experts visualize unavoidable physiological data from distant regions. "The Internet of Things (IoT) is a proven concept that, with the help of wireless sensor networks (WSN), intends to enhance all those services and devices that drastically cut down on human mediation and ensure a higher quality of life [5, 6]. Information collected by wearing sensors may be made readily available at any time and place thanks to a wireless sensor network enabled by the Internet of Things (IoT). To keep up with the constant monitoring of human vital limits, a vast data storage facility is necessary." The GSMA estimates that by 2020 there will be 24 billion connected wearable devices, up from 7 billion in 2015 [7] and 8 billion in 2020 [8]. A synchronised processing device that has an Internet connection may improve the quality of medical treatment that is provided to patients in a clinic or other setting that simulates a home environment. The major testing functions of WSN in medical clinics are security, sensor position, neatness, security, & [9] care giving information. For all WSN applications [10], the effective transmission of aggregated data along the base is delayed from start to finish. This can be accomplished through incorporating agreed & network-coded correspondence into the current WSN [11] [12].This study is arranged as follows: in part 2, a description of the literature review; in section

3, a description of the comparative study analysis; in section 4, a Research Gap analysis; and in section 5, a description of the final conclusion.

2. Literature Review

This section provides a high-level overview of the problem of cyber security assaults and the means by which they may be avoided. Recent advances are discussed, along with the researchers' involvement and contributions.

In [13] the identification labels for SNs are generated with the help of a hash technique, and a trust evaluation model is constructed using the beta density function as its foundation.

The authors of the paper [14] offer multidimensional trust indicators that are obtained from communication between neighbouring sensor nodes.

In [15], the authors offer a fuzzy-based hierarchical trust management scheme. This system combines direct trust calculation based on real-time previous experience and credit-based calculation, as well as indirect trust calculation based on peer endorsement. In this particular plan, CH and BS were responsible for maintaining a constructive knowledge table that was based on fuzzy logic, which helped to decrease the amount of memory and communication overhead.

For the purpose of providing safe routing in WSNs, the authors of [16] suggest a Trusted Tree-based trust management system. The most prevalent forms of assault were initially scrutinised. And then, under the distributed trust model, a dynamic time frame was established, which included the detection of direct trust as well as indirect trust. The Trustworthy Tree had been developed on the basis of the trusted nodes. And the gradient that was utilised for routing was determined by the route quality of the nodes in the Trusted Tree.

In the article [17], the author suggested a trust scheme for clustered WSNs that were both lightweight and reliable. Because it eliminates feedback between nodes, it has the potential to significantly boost system efficiency while simultaneously diminishing the impact of malicious nodes. When it comes to collaboration amongst CHs, using a dependability-enhanced trust assessing technique may successfully identify and avoid the behaviour of CHs that are malevolent, self-cantered, or flawed.

An effective and economical distributed trust model for WSNs has been presented by the authors of [18]. In situations in which a subject node is unable to directly see the communication behaviours of an object node, the subject node will instead acquire an indirect trust value based on the recommendations of other nodes.

In [19], a strategy for the building of trust that was both lightweight and resilient and that used the weight of misbehaviour was presented. Their plan includes the implementation of a brand new trust component called misbehaviour frequency in order to increase the robustness of the trust mechanism.

A trust-based intrusion detection technique was given by the author in [20]. They use honesty as a measurement of social trust, as well as energy and cooperation as a measurement of the trustworthiness of service quality.

In [21-23], haves have offered several unique strategies. Intimacy, honesty, selflessness, and vitality were the four main aspects of trust that were taken into consideration.

The authors of [24] suggest a physical layer intrusion detection system (IDS) as a means of delivering security at the physical layer. This approach is limited to identifying a denial of service attack that is caused by a jamming assault. The MAC layer and the network layer both have insufficient and no security.

The cross-layer method has been presented by the authors in [25] for the purpose of attack detection in MANET and WSN. They devised a method that consists of two levels of detection in order to identify malicious nodes in MANETs. At the beginning of the game, specialised sniffers operating in promiscuous mode are deployed. Every sniffer makes use of a classifier based on a decision tree, which, at each reporting time, produces a certain quantity of what are known as correctly classified

instances (CCIs).

For the purpose of countering cross-layer security assaults in wireless networks, a new framework known as FORMAT was presented in reference [26]. The FORMAT included of a detection component as well as a mitigation component, and it was based on Bayesian learning. On the one hand, the component responsible for attack detection builds a model out of the information that has been seen in order to identify covert attack actions. The optimization theory is used by the mitigation component in order to establish the optimal balance that is required between performance and security.

The model was built on a cross-layer technique that was described in [27] to identify sinkhole attacks in wireless sensor networks (WSNs). The author is responsible for the creation of both the detection and prevention algorithms.

In [28], the author explains that the present layers of security solutions are typically wasteful and ineffective because of problems like the duplication and/or inflexibility of the security solutions. "Redundancy and/or rigidity in the security measures used by layered systems are often cited as the causes of these problems. Considering this, it is beneficial to construct the WSNs' security strategy on the basis of the cross-layer interaction between all of the components in the different tiers of the protocol stack." This will contribute to the safety of the WSNs.

In [29], rather of using a monolithic cross-layer approach, the author used a component-based design. "He also looked at template meta-programming approaches to alter and recombine primary building blocks." An event-driven framework that employs zero-copy buffers and metadata for solving problems that cut across disciplines.

It has been shown in reference 112 that the Elliptic Curve Digital Signature Algorithm (ECDSA) may be used in an application that spans many layers of a protocol this is shown in [30]. Data transit and access control are both made more secure by the lightweight secure system's use of a proxy signature approach based on ECDA.

In [31] this framework was intended to identify attacks on wireless sensor networks. They developed a trust-based intrusion detection technique for protocol layers of wireless sensor networks. The author focused primarily on considering these three facets of trustworthiness: the trustworthiness of the physical layer, the trustworthiness of the media access control layer, and the trustworthiness of the network layer. After that, the individual trust measures for each layer are added together to provide an overall trust metre for a sensor node.

A more current proposal for a cross-layer trust-based attack detection technique may be found in reference [32]. The strategy outlined in is conceptually comparable to this approach. Taking into account the most important trust metrics of a given layer allows one to determine how trustworthy a sensor node is at a certain layer. In the last step, the individual trust values of each layer are combined to arrive at an estimate of the total trust value of the sensor node. When the trust threshold is applied, it is possible to determine whether or not a sensor node should be trusted.

The authors of [33] created an intrusion detection system that is based on the cross-layer interaction that occurs between the network and MAC levels of the OSI model. XLID was validated in comparison to typical (non-cross-layered) intrusion detection systems (IDS), which are based on single-layer protocols.

The author presents a strategy to limit the impact of sinkhole attacks on networks by making use of the cross-layer methods in [34]. In order to improve the network's overall security, the activities that take place at the network and MAC layers are combined. The suggested research will hunt out the rogue node in the network by measuring the intensity of the signal and identifying each node.

3. Comparative analysis

Ref. No	Author name	Year	Methods	Objectives
35	Cabaj et al.,	2016	A well-known classification of the security strategies for classical computer systems is: (i) Prevention, (ii) Detection, and (iii) Recovery	Preventive measures that prevent the attackers from tampering with communication messages, e.g., like encryption and authentication. Detective measures that perform anomaly detection during protocol executions and alerts when it exceeds certain tolerance level.
36	Chamotra, S, al.,	2011	The paper that follows will provide an overview of the several detection methods currently in use for replication attacks.	Both centralised and distributed systems have the same overarching goal, which is to have nodes make location claims that identify their positions and seek to discover contradicting reports that indicate the same node in various places.
37	Xu, Ning, et al.,	2004	This algorithm creates exclusive unit subsets among one-hop neighbours in an only one disjoint subset. These exclusive unit subsets are controlled by a randomly determined leader.	According to this plan, the network would be split up into sub regions. After ensuring that every node in each sub-region is a one-hop neighbour of every other node in the sub-region, the head of the sub-region is chosen.
38	He, Tian, et al.,	2004	There is a potential for a failure at a single location using this strategy. In addition, the communication overhead that is required for these sub-area duplicate detection approaches is much too high.	According to their plan, the central node will be chosen from among the nodes based on the highest number of neighbours each has. After then, the whole network is divided up into smaller sections called sub-areas. Every sub-region is situated in the exact same location around the head node.

39	Akyildiz, et al	2002	A strategy for detecting clones was suggested in reference to random key pre-distribution in the article	The purpose of this is to identify keys that are accessible on cloned nodes by monitoring how often they are used to authenticate the node in the network. In this scenario, every node performs a counting bloom filter on the keys that are issued to interact with the nodes that are nearby, and then appends its own count to the result.
40	Nadeem, et al.,	2015	The use of randomization is one of the main factors in witness finding technique in order to prevent the prediction of future witnesses.	If the adversary was aware of future witnesses, they may manipulate the nodes in the network in a manner that would prevent the attack from being uncovered. However, there is a chance that a malicious node will be picked as a witness owing to the random nature of the selection process.

4. Research Gap analysis

The layered trust-based mechanism for attack detection WSN failed to detect the cross-layer attacks like MIMA. The main concern of the cross-layer protocols was the detection of a variety of attacks using the cross-layer characteristics of each sensor node in WSNs, with or without an examination into performance. The inability to properly optimise resources using this method in the absence of an effective clustering mechanism for WSNs is the cause of the issue. When compared to other kinds of routing algorithms, clustering has previously been shown to be a more energy-efficient option for resource-limited WSNs. Provide cross-layer solutions that are not vulnerable to the numerous issues provided by WSNs, such as the maintenance of data security and privacy. The goal of the research into cryptography-based solutions was to provide privacy preservation in wireless sensor networks (WSNs). But these solutions aren't without their problems, such the fact that some of them simply concentrate on privacy protection and don't bother with clustering at all. A few of the approaches did not take into account the trustworthy relay selection required for safe data transfers.

5. Conclusion

The node replication attack has hazardous impacts on WSN and its security goals. This chapter deals with various existing detection, prevention and recovery approaches for node replication attack. Additionally, the study organises the several available mitigation techniques and evaluates their

benefits and drawbacks. A centralised and decentralised taxonomy of techniques for detecting node replication attacks has been proposed for both WSN and MWSN. In particular, two variants of the node replication assault, the smart attack and the masked replication attack, may bypass the existing distributed witness node based detection systems. These kinds of assaults create a weakness in the detection systems in question. When compared to other networks, healthcare applications provide a larger difficulty for ensuring the security and privacy of sensitive information owing to the restricted processing capacity and battery life of sensor devices. We have studied the various research works for security in IoT enabled applications using WSNs in this paper.

References

[1] Kore, A., Patil, S. IC-MADS: IoT Enabled Cross Layer Man-in-Middle Attack Detection System for Smart Healthcare Application. Wireless PersCommun 113, 727–746 (2020). https://doi.org/10.1007/s11277-020-07250-0.
[2] Gilbert, E. P. K., Baskaran, K., Rajsingh, E. B., Lydia, M., &Selvakumar, A. I. (2019). Trust aware nature inspired optimised routing in clustered wireless sensor networks. International Journal of Bio-Inspired Computation, 14(2), 103. doi:10.1504/ijbic.2019.101637.
[3] Haseeb, K., Islam, N., Almogren, A., Din, I. U., Almajed, H. N., &Guizani, N. (2019). Secret Sharing-based Energy-aware and Multi-hop Routing Protocol for IoT based WSNs. IEEE Access, 1–1. doi:10.1109/access.2019.2922971.
[4] Alghamdi, T. A. (2018). Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method. IEEE Access, 1–1. doi:10.1109/access.2018.2865909.
[5] Kanoosh, Huthaifa&Houssein, Essam&Selim, Mazen. (2019). Salp Swarm Algorithm for Node Localization in Wireless Sensor Networks. Journal of Computer Networks and Communications. 2019. 1-12. 10.1155/2019/1028723.
[6] Sharma, R., Vashisht, V., & Singh, U. (2020). eeTMFO/GA: a secure and energy efficient cluster head selection in wireless sensor networks. Telecommunication Systems. doi:10.1007/s11235-020-00654-0.
[7] Rodrigues, P., John, J. Joint trust: an approach for trust-aware routing in WSN. Wireless Netw (2020). https://doi.org/10.1007/s11276-020-02271-w.
[8] Ramesh, S., &Yaashuwanth, C. (2019). Enhanced approach using trust based decision making for secured wireless streaming video sensor networks. Multimedia Tools and Applications. doi:10.1007/s11042-019-7585-5.
[9] Mabodi, K., Yusefi, M., Zandiyan, S. et al. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. J Supercomput 76, 7081–7106 (2020). https://doi.org/10.1007/s11227-019-03137-5.
[10] Agarwal, M, Biswas, S & Nandi, S 2015, 'Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach,' in Proc. of IEEE International Conference on Systems, Man, and Cybernetics, pp. 246 - 251.
[11] Agarwal, M, Purwar, S, Biswa, S & Nandi, S 2017, 'Intrusion detection system for PS-Poll DoS attack in 802.11 networks using real time discrete event system,' in IEEE/CAA Journal of AutomaticaSinica, vol. 4, no. 4, pp. 792-808.
[12] Alazab, A, Hobbs, M, Abawajy, J &Khraisat, A 2013, 'Malware Detection and Prevention System Based on Multi-Stage Rules', International Journal of Information Security and Privacy (IJISP), vol. 7, no. 2, pp. 29-43.
[13] Wenbo Zhang ; Ling Li ; Guangjie Han ; Lincong Zhang, "E2HRC: An Energy-Efficient Heterogeneous Ring Clustering Routing Protocol for Wireless Sensor Networks", IEEE Access (Volume: 5), 2017

[14] PeymanNeamatollahi, Mahmoud Naghibzadeh, SaeidAbrishami, Mohammad-Hossein Yaghmaee,"Distributed Clustering-Task Scheduling for Wireless Sensor Networks Using Dynamic Hyper Round Policy", IEEE TRANSACTIONS ON MOBILE COMPUTING, TMC-2016-02-0080, 2017
[15] Han, G., Zhou, L., Wang, H., Zhang, W. and Chan, S. (2017), 'A source location protec- tion protocol based on dynamic routing in wsns for the social internet of things', Future Generation Computer Systems 82(1), 689–697.
[16] Qiu, T., Lv, Y., Xia, F., Chen, N., Wan, J. and Tolba, A. (2016), 'Ergid: An efficient routing protocol for emergency response internet of things', Journal of Network and Computer Applications 72(1), 104–112.
[17] Lee, I.-G. and Kim, M. (2016), 'Interference-aware self-optimizing wi-fi for high effi- ciency internet of things in dense networks', Computer Communications 89(1), 60–74.
[18] Qiu, T., Luo, D., Xia, F., Deonauth, N., Si, W. and Tolba, A. (2016), 'A greedy model with small world for improving the robustness of heterogeneous internet of things', Computer Networks 101(1), 127–143.
[19] Shen, J., Wang, A., Wang, C., Hung, P. C. and Lai, C.-F. (2017), 'An efficient centroid- based routing protocol for energy management in wsn-assisted iot', IEEE Access 5(1), 18469–18479
[20] Mahajan, S., Malhotra, J. and Sharma, S. (2014), 'An energy balanced qos based cluster head selection strategy for wsn', Egyptian Informatics Journal 15(3), 189–199.
[21] Khan, B. M., Bilal, R. and Young, R. (2017), 'Fuzzy-topsis based cluster head selection in mobile wireless sensor networks', Journal of Electrical Systems and Information Technology 4(3), 89–101.
[22] Wang, W., Hu, L. and Li, Y. (2010), 'Security analysis of a dynamic program update protocol for wireless sensor networks', IEEE Communications Letters 14(8), 782–784.
[23] Ke, W., Yangrui, O., Hong, J., Heli, Z. and Xi, L. (2016), 'Energy aware hierarchical cluster-based routing protocol for wsns', The Journal of China Universities of Posts and Telecommunications 23(4), 46–52.
[24] Oladimeji, M. O., Turkey, M. and Dudley, S. (2017), 'Hach: Heuristic algorithm for clustering hierarchy protocol in wireless sensor networks', Applied Soft Computing 55(1), 452–461.
[25] Kannan, G. and Raja, T. S. R. (2015), 'Energy efficient distributed cluster head schedul- ing scheme for two tiered wireless sensor network', Egyptian Informatics Journal 16(2), 167–174.
[26] Shankar, T., Shanmugavel, S. and Rajesh, A. (2016), 'Hybrid hsa and pso algorithm for energy efficient cluster head selection in wireless sensor networks', Swarm and Evolutionary Computation 30(1), 1–10.
[27] Song, L., Chai, K. K., Chen, Y., Schormans, J., Loo, J. and Vinel, A. (2017), 'Qos- aware energy-efficient cooperative scheme for cluster-based iot systems', IEEE Systems Journal 11(3), 1447–1455.
[28] Xu, Z., Chen, L., Chen, C. and Guan, X. (2016), 'Joint clustering and routing design for reliable and efficient data collection in large-scale wireless sensor networks', IEEE Internet of Things Journal 3(4), 520–532.
[29] Sirdeshpande, N. and Udupi, V. (2017), 'Fractional lion optimization for cluster head- based routing protocol in wireless sensor network', Journal of the Franklin Institute 354(11), 4457–4480.
[30] Rehman, E., Sher, M., Naqvi, S. H. A., Badar Khan, K., & Ullah, K. (2017). Energy efficient secure trust based clustering algorithm formobile wireless sensor network. Journal of Computer Networks and Communications, 2017, 1630673.
[31] Mittal, N. (2019). Moth flame optimization based energy efficient stable clustered routing approach for wireless sensor networks. Wireless Personal Communications, 104(2), 677–694.

[32] Sharma, R., Vashisht, V., & Singh, U. (2019). Nature Inspired Algorithms for Energy Efficient Clustering in Wireless Sensor Networks. 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). doi:10.1109/confluence.2019.8776618.
[33] Sharma, R., Vashisht, V., & Singh, U. (2019). EEFCM-DE: Energy Efficient Clustering Based on Fuzzy C Means and Differential Evolution Algorithm in Wireless Sensor Networks. IET Communications. doi:10.1049/iet-com.2018.5546.
[34] Pavani, M., &Trinatha Rao, P. (2019). Adaptive PSO with Optimized Firefly Algorithms for Secure Cluster Based Routing in Wireless Sensor Networks. IET Wireless Sensor Systems. doi:10.1049/iet-wss.2018.5227.
[35] Cabaj, K &Mazurczyk, W 2016, 'Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall,' in IEEE Network, vol. 30, no. 6, pp. 14-20
[36] Chamotra, S, Bhatia, JS, Kamal, R &Ramani, AK 2011, 'Deployment of a low interaction honeypot in an organizational private network,' International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Udaipur, pp. 130-135.
[37] Xu, Ning, SumitRangwala, Krishna Kant Chintalapudi, Deepak Ganesan, Alan Broad, Ramesh Govindan, & Deborah Estrin. "A wireless sensor network for structural monitoring." In Proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 13–24. ACM, 2004.
[38] He, Tian, Sudha Krishnamurthy, John A. Stankovic, Tarek Abdelzaher, Liqian Luo, RaduStoleru, Ting Yan, Lin Gu, Jonathan Hui, & Bruce Krogh. "Energy-efficient surveillance system using wireless sensor networks." In Proceedings of the 2nd international conference on Mobile systems, applications, & services, pp. 270–283. ACM, 2004.
[39] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, &ErdalCayirci. "Wireless sensor networks: a survey." Computer networks 38, no. 4 (2002): 393–422.
[40] Nadeem, Adnan, Muhammad Azhar Hussain, ObaidullahOwais, Abdul Salam, Sarwat Iqbal, & Kamran Ahsan. "Application specific study, analysis & classification of body area wireless sensor network applications." Computer Networks vol. 83, pp. 363–380.2015.