ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse78842019.pdf
https://doi.org/10.30534/ijatcse/2019/78842019

Security Issues and Challenges on Wireless Sensor Networks

Muawia A. Elsadig[1], Abdulrahman Altigani[2], Mohammed Abuelaila Ali Baraka[3]
[1] Deanship of Scientific Research, Imam Abdulrahman Bin Faisal University P.O. Box 1982, Dammam, Saudi, muawiasadig@yahoo.com
[2] Deanship of Graduate Studies, Imam Abdulrahman Bin Faisal University P.O. Box 1982, Dammam, Saudi, aaaltigani@iau.edu.sa
[3]College of Applied Studies and Community Service, Imam Abdulrahman Bin Faisal University P.O. Box 1982, Dammam, Saudi Arabia, maabaraka@iau.edu.sa

ABSTRACT

Wireless Sensor Networks (WSNs) are emerging as a rich field of active research that is involved different aspects. Nowadays, sensors are used in many domains as applications that can monitor and control. These domains include applications such as environmental, home, commercial, military, health, etc. WSNs are used in numerous applications that involves sensitive information needs to be secure and confidential. Especially in applications that deal with top secret information such as military applications. Therefore, the important of security issues in WSNs have received potential attention from designers, developers, and security professionals. Moreover, this type of network is highly vulnerable to numerous security attacks due to its resource constraints and mobility. This paper gives comprehensive details in WSN constraints, vulnerabilities, and security attacks. In addition, the paper investigates the recent countermeasures that are used to counter WSN attacks in terms of their achievements and limitations. The paper concludes that security is the key to success for WSN applications, However, still many critical security problems are remained unsolved. Moreover, when designing an adequate security solution; productivity, usability, mobility, resource constraints and privacy preservation should all be taken into account. Therefore, a huge challenge still facing researchers and designers to bring up sufficient solutions to secure WSN applications.

Key words: Wireless Networks, Wireless Sensor Networks, WSNs, Sensor Nodes, WSN applications, Security Attacks, Underwater WSNs, Body Sensor Networks, Cluster WSNs, Intrusion detection; Sensor Node attacks; Denial of Service.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have been gaining a lot of attraction from the research community due to their important contribution to different applications in general life. Sensors applications are categorized into two main categories; (i) tracking and (ii) monitoring [1]. In which these applications are include business, military, habitat, industrial, health, public, and environmental. Nowadays, WSNs could be exist in different forms such as underwater, underground, terrestrial, and multimedia WSNs. The initial motivation behind the desire to advance and develop research in WSNs had been triggered by military applications. The reason is due to the fact that WSNs have large arrays of distributed sensors that could be used instead of high-cost sensor assets [2].

WSN has a great potential in constructing a new generation of distributed system. However, this type of networks is different than the traditional networks. It faces much more challenges. Security issues and energy efficiency are considered as the most critical challenges that face WSN systems [3]. In terms of security, Denial of Service (DoS), node damage, node duplication are considered as mainstream attacks [4]. Interested readers on energy efficiency are referred to [5].

Xiangqian et al. [6], drawn attention to show the important of data assurance, survivability, security assessment, trust evaluation, security and privacy support, end-to-end security, and node compromise distribution in sensor network security. They mentioned that only few approaches are available in this regard, therefore, the research door is still open for more research in these aspects.

WSNs are typically more vulnerable to numerous security attacks as this type of networks is used the unguided transmission medium which is highly vulnerable to different security threats. Moreover, eavesdropping is easily to be occurred because of the broadcast communication of wireless networks [7]. Generally, the wireless medium makes WSNs vulnerable for an attacker to jam communication, eavesdrop, or inject messages into the network system [8]. On the other hand, the limitations in computing power, memory and battery in sensor networks make many security algorithms inapplicable to be used in such networks such as public key cryptography.

Although numerous of research proposals and approaches have been conducted concerning security in WSNs, but an adequate security solution still a hot issue and demanding task. WSNs have a great potential to be used in numerous applications therefore, recently, this type of networks has received much attention especially on maintain adequate way to keep data secure and confidential in order to obtain a constructive secure network that benefits all kind of applications. In fact, the advances in wireless technologies and the rapid growth of wireless network services have encourage many different domains to use wireless communications as a common medium for information transferring across their networks [9]; therefore, the security in such networks is an important issue.

This paper gives comprehensive details in WSN constraints, vulnerabilities, and attacks. The core of the paper is to investigate the recent WSN attack countermeasures and evaluate their achievements and limitations. The paper is organized as follows: the first section has defined the WSNs and gives brief introduction about their applications, constrains, attacks, and security. Section 2 lists the security requirements that should be satisfied in order to archive the goals which aim to attain secure WSN applications. Section 3 sheds lights on WSN attack types and their classifications. Subsequently Section 4 gives a thorough investigation on WSN countermeasure approaches and mechanisms. It discusses their achievements and limitations. Finally, the conclusion and future work are summed up in Section 5.

2. GOALS

To achieve security on WSNs, all the following issues should be taken into account and should be achieved. These issues involve confidentiality, integrity, availability, non-repudiation, authentication, accountability, and freshness. In addition, two more issues also are considered important to attain secured WSNs, these issues are (i) forward secrecy and (ii) backward secrecy [6].

Even though the security objectives of traditional wired networks and WSNs are the same, which in general, these objectives include maintain confidentiality, integrity, availability, non-repudiation, and authentication, however, the WSN security issues, to some extent, are quite different.

3. WSN ATTACKS CLASSIFICATION

Due to their broadcast nature and their nodes are often located in a dangerous or hostile environment that is hard to be protected, WSNs are highly vulnerable to many security attacks.

In literature, they are many ways have been followed to classify WSN attacks such as active vs. passive, insider vs. external and layer-based classification. Marzi and Marzi [10], classified the attacks into (5) classes that include wormholes, selective forwarding, Sybil, sinkhole, and HELLO flood attacks.

The following two subsections focus on two types of WSN attack classifications. The layered-based classification and the internal\external classification. Interested readers on passive vs. active attacks classification are referred to [11].

3.1 Internal/External Classification

Table 1 classify WSN attacks into insider (internal) and outsider (external) attacks [12]. Interested reader for more information on insider and outsider attacks is referred to [13].

Table 1: WSN Internal/Eternal Attacks Classification [12].

Internal	External	Internal /External
Collision	Eavesdropping	Node tampering
Replay attack	Basic jammers	Hardware hacking
Selective forwarding	Intelligent jamming	Spoofed/altered inf.
Black hole	Node replication	Hello flood
Sinkhole		Energy drain
Sybil attack		Desynchrony attak
Worm hole		Attack on reliability
Data integrity		Malicious code attack
		Denial of service
		Man in the middle

This classification reflects that high number of the inside attacks in comparison with the external attacks.

3.2 Layer-based Classification:

Kavitha and Sridharan [14] took the direction to classily WSNs attacks based on the WSN layers (a layer-based classification) and also based on other aspects. This paper sheds lights on layer-based classification. Table 2. summarizes this classification.

Table 2: Layer-Based Attacks Classification [14].

Layer	Attack Types
Physical Layer	Tampering /destruction, Radio interference, Jamming
Data Link Layer	Unfairness, Collision, Exhaustion, Interrogation, Sybil Attack.
Network Layer	Node Capture, Sybil, Sinkhole, Selective Forwarding / Black Hole [15-17], Hello Flood, Wormhole, (Altered, spoofed or Replay Routing Information), Acknowledgment Spoofing, Homing, Internet Smurf, Misdirection
Transport Layer	De-synchronization, flooding
Application Layer	Path-based DOS, overwhelm, deluge

Based on the above classification, it is clearly noticeable that the number of network layer attacks is dominant compared to other layers. Figure 1 below reflects the high number of attacks that work on network layer level.

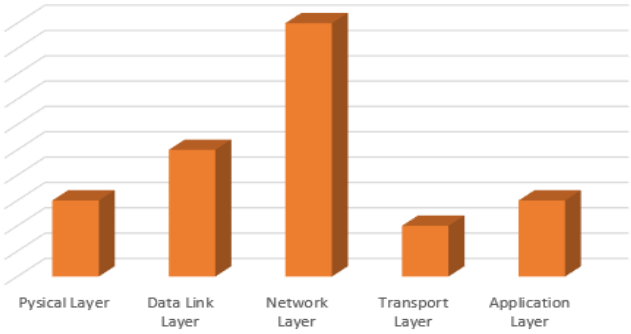

Figure 1: Percentage of attacks targeting each WSN layer

4. RELATED WORK

This section, in terms of their achievements and limitations, investigates the recent countermeasures that are used to counter WSN attacks. It covers different types of WSNs such as Clustered Wireless Sensor Nodes (CWSNs), Under Water Sensor Networks (UWSNs), body sensor networks, etc. with closely focus on some dangerous and common WSN attacks.

Schaffer et al. [18] pointed out the importance of clusters wireless sensors networks (CWSNs) and their security. They gave a review on security and reliability issues in CWSNs and they proposed countermeasures against their Attacks.

Lu et al. [19] have pointed out the deficiency of symmetric key management to maintain secure data transmission as it suffers from orphan node problem. Instead, the authors proposed two data transmission protocols for Clustered Wireless Sensor Nodes. These two protocols are SET-IBS and SET-IBOOS. The key idea is to authenticate the encrypted sensed data using digital signatures. The authors stated that the two proposed protocols can achieve security requirements in CWSNs better than the existing protocols. Their model, as well, can solve the orphan node problem. However, the generation of the key is computationally expensive and that would limit the Key strength and the dynamic structure of the network [20]. In addition, the SET-IBS gives an acceptable solution for passive and active attacks; however, the network lifetime is still an issue due to the asymmetric cryptography computational overhead [21].

As there are many applications that are based on WSNs, the improvement of security and reliability is become a vital requirement. The trust management systems - that are used in large scale WSNs - fail due to their low dependability, memory overheads and higher communication [22]. Therefore, Khan et al. [22] introduced trust estimation approach for large scale WSN (LTS). The proposed approach (LTS) claims its feasibility to enhance security through its capability to detect and mitigate malicious nodes. However, LTS is not recommended to be used for mitigation of collusion and on-off attacks as the authors stated. In addition, the other limitation is that the LTS is closely suitable for homogeneous WSNs.

Osanaiye et al. [23] introduced statistical detection approach to detect WSNs DoS jamming attack. DoS jamming attack disrupts and interferes the normal functions of WSNs. It generates radio frequency signals to jam legitimate signals in order to cause a denial of service. The proposed detection approach works at the base station and the cluster head to detect attacks in cluster heads and member nodes respectively. The proposed approach claims its capability to detect the presence of jamming attack efficiently and it is adequate to be implemented for real time applications. However, for more trust on this approach, the approach needs to be evaluated using different datasets that consider more different scenarios.

Nguyen et al. [24] discussed some jamming attacks and concluded that no effective and holistic antijamming method is presented to defeat them. In addition, the authors pointed out that energy depletion attacks (EDA) are still considered as real threats especially in sensor networks that are used for critical infrastructures. EDA is a resource depletion attack that causes high damage to the applications in which network availability is important [25].

Wireless power transfer (WPT) is a breakthrough in wireless which help to minimize the problem of energy limitation in WSNs. Accordingly, the concept of Wireless Rechargeable Sensor Network (WRSN) has attracted many researchers and

developers. Recently, much efforts have been paid to enhance WRSN performance through optimizing the charging scheduling. As a result, many researches pay more attention on scheduling algorithms, system performance and collaborative control without taking into consider the security issues. As an example, if many charge requests are received from malicious nodes, wrong charging response may happen, and this may lead to prevent many legitimate charging requests from charging services. In this case a Denial of Charge (DoC) attack will happen which leads to destruct network functionality and reliability [26]. In this context, Lin et al [26] developed a Collaborative Denial of Charge attack algorithm (CoDoC) which generates fake charging requests. The authors pointed that, the CoDoC outperforms in making sensor exhausted and causes missing events. This shows the highly need from security professionals, designers and developers to pay much attention to WRSNs security issues.

It is commonly known that the routing protocol and its components are crucial part of WSNs. However, the routing protocol is highly vulnerable to Low-rate Denial of Service (LDoS) attack. In fact, the existing traditional intrusion detection methods are incapable to detect this attack; therefore, LDoS attack represents a real challenge for WSNs [27].

Sybil attack is one of the WSN dangerous attacks in which malicious node simultaneously propagates multiple forged identities. In this context, Jamshidi et al. [28] introduced a sybil attack to target CWSNs. In which, a malicious node can join many clusters at the same time by using one of its Sybil identities. This Sybil attack is different than the attack model proposed by Chen et al. [29] where a malicious node acts as a cluster head. If each Sybil ID becomes a cluster head this leads to extraordinary number of cluster heads. In this case, the sink node can detect this situation easily and thus detect the occurrence of the attack. This is the reason why a malicious node in the Jamshidi et al. proposed attack does not try to be a cluster head [28]. Although the authors introduced a method against this attack, but this reflects the ongoing developments of WSN attacks and how much the needed efforts from security professionals to stand against these developed attacks.

Kukreja et al. [30] proposed a method to secure Mobile Ad Hoc Networks. Their method is to add some security enhancements to Dynamic Source Routing protocol (DSR). Their enhanced protocol is called Security Enhancement Dynamic Source Routing (SE-DSR). It selects the most trusted path between source node and destination node that has no malicious nodes in between. SE-DSR is capable to detect the following nodes misbehaviors: network topology change, packet modification and selfish. In contracts with the other protocols that require all nodes to work as promiscuous nodes, the enhanced protocol is only used few numbers of nodes to work as promiscuous nodes and thus will decrease the network overheads. However, in this case, a high energy capacity is required for the promiscuous nodes which are overhearing the transmission of all nodes within their range in order to detect any malicious node.

Numerous techniques have been proposed for black hole attack detection and prevention in WSNs, However, these techniques are suffered from very little false positives [15]. Most of the techniques in non-WSNs are not suitable to be applied to the black hole problem in WSNs. That is due to the WSN constraints [15].

Yuanpeng et al. [31] introduced a new framework of combining WSNs and cloud computing. Cloud computing can effectively help in solving some WSNs issues such as storage limit, accessibility, etc. but the vulnerabilities and security issues still exist. The security challenges of the proposed framework were analyzed, and some solutions were given accordingly to overcome these issues; however, still many challenges are remained unsolved.

Although there are some security technologies that have been investigated to get Under Water Sensor Networks (UWSNs) secured, most of them are still in their theory phase. Yang et al. [32] introduced a comprehensive work in security issues, challenges, attacks, constraints of UWSNs. They stated that security research regarding UWSNs is still in its early stage and more security issues are not yet meet their adequate solutions. In fact, UWSNs has some special particularities and constraints that complicating the way to attain sufficient security solutions with an acceptable overhead. In addition, Yang et al. addressed that many WSN security approaches are not applicable to UWSNs. As an example, synchronization security protocols that proposed for WSNs are unstable for UWSNs as well as the countermeasures against WSNs delay attack that introduced in [33-35] are not applicable for UWSNs. The readers are referred to [32] for more details in UWSNs particularities and constraints.

As all wireless networks, WSNs are vulnerable to covert channel attacks [36]. A covert channel is a communication channel that is used for illegal flow of information in a manner that violates system security policy. It is invisible, undetectable and dangerous, security attack [37, 38]. Moreover, Swaminathan and Vivekanandan [39] stated that; nowadays, the covert communication in WSNs become popular and emerging problem. Interested readers in covert channels are referred to [40-42].

A framework for sensor security application development (Monitoring Core) was developed and tested [43]. The service-oriented architecture of the aforementioned

framework facilitates and accelerates the development of security applications for WSNs. Moreover, the authors of this framework have developed a new language to facilitates the use of the monitoring framework. The framework and its supported language along with five security applications had been implemented and tested on real sensors. However, further evaluation and testing are required for both the framework and the language especially after increasing the number of the Monitoring Core services.

Policy system to support adaptability and security on body sensor networks has been proposed in [44]. The authors mentioned that their model had been implemented and evaluated successfully on body sensor networks. However, this model is not yet implemented on the other types of WSNs. Moreover, the authentication module still needs to be integrated and thus the complete proposal needs to be implemented and evaluated. There are many approaches applied public key cryptography to Wireless Body Area Networks (WBAN) such as [45, 46]. While other approaches, to avoid the overheads of establishing the public key infrastructure, they took different direction by using identify-based cryptography such as the approaches in [47, 48]. Even though, identify-based cryptography is a certificateless cryptography (where no need for digital certificate), it is unsecure when the Key Generation Center (KGC) is invalid [49]. Interested readers on WBAN are referred to [50-53].

Uppuluri and Basu [54] presented a novel multi-layer framework. They claimed that this framework can protect integrity and confidentiality of data stored in sensors. It secures TinyOS against both unknown and known attacks. In case of repeated attacks, the sensor destruct itself prior any attempt to compromise its data. However, the multi-layer framework is yet to be deployed in sensor networks as well as its efficiency is yet to be measured in terms of battery consumption.

An Agent-based Trust Model (ATSN) for WSNs have been proposed in [55]. In ATSN, each agent node watches the behavior of other nodes that exist on its radio range, and then the agent node broadcast the rating of trust of these nodes. As the authors claim, this scheme helps in limiting malicious attack effect. Attacks such as conflicting behavior attack, on-off attack, and bad-mouthing attack. Their proposed scheme assumes that the agents are trusted third parties that they would not engage in ballot-stuffing or bad-mouthing attacks [56] [57].

Marzi and Marzi [10] proposed an Enhanced bio-inspired trust and reputation system, EBTRM. Their proposed system is inspired by the existing approaches: (i) Peer Trust system and (ii) Bio inspired Trust and Reputation System BTRM-WSN. The objective behind the proposed system (EBTRM) is to enhance WSNs security and to keep the energy consumption at its lowest possible level. The authors stated that, their enhanced model has gained highest performance compared to the aforementioned two systems. However, to trust this result, more simulations are needed to be implemented in different sizes of networks as well as to implement simulations using different trusted simulation tools.

Traditionally, cryptographic mechanisms are the common schemes that are used for security in WSNs, whereas this traditional scheme covers some parts of security issues that WSNs can faces. As an example, nodes can be physically captured and thus, enemy can use them in order to insert or inject false data to the entire network and consequently this leads to different damages that may affect the entire network such as disturbing communications among network nodes. Haiguang et al. [9] stated that cryptographic and authentication mechanisms such as INSENS, SERP, Key session Scheme, TinySec, SPINS, etc. are not sufficient to be used alone.

In military applications, a secure channel must be used to exchange critical information in real time and to maintain privacy. WSNs have important role to play in such applications but, as we know, WSNs is highly vulnerable to numerous security threats such as node capturing eavesdropping, man in the middle, etc. Gupta et al. [58] mentioned that in order to ensure security, all messages over WSNs must be encrypted. They stated that many key agreement approaches were proposed to ensure that the system is secured but unfortunately most of them are quite complex. Therefore, Gupta et al. proposed a pre key distribution scheme for public key cryptography to be applicable for military applications. As the authors stated that their proposed scheme can enhance performance in terms of memory usage, resource consumption, scalability, resiliency against node capturing, resistant against node, etc. However, using of public key may not considering cost.

WSNs are characterized by low bandwidth, small memory sizes, limited power supplies, therefore an adequate security mechanism should be applied accordingly. Furthermost security approaches implement symmetric key cryptography and thus presenting complex key management. On the other hand, in spite of the fact that public key is too expensive with regard to energy cost and computation, some recent approaches show the availability of public key cryptography to be adopted in WSNs by selecting appropriate algorithms, parameters, etc. [59] [60] but these trends still need further studies [6]. Using any encryption structure needs transmission of further bits, therefore, this means extra processing [7]. Applying encryption mechanism lead to

increase delay, jitter and packet loss in this type of network [61]. Therefore, the type of the security mechanism in WSNs need to be adequately chosen and adopted to fulfil the security requirements.

We do believe that one of the solutions the researchers can think about to obtain sufficient security for WSNs is to benefit from the advanced technology in designing devices that can deliver high speed, fewer cost value, fewer energy consumption and enable adequate storage space. Panic et al. [62] introduced a low power sensor node microcontroller that takes into account the WSN security issues. The authors claimed that their design is sufficient to enable efficient execution of some advanced security algorithms such as Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm. In addition, their design can also enable robust wireless communication and supports direct sequence spread spectrum (DSSS).

Jaydip Sen [63] highlighted that although there are great research efforts that done on key management, cryptography, intrusion detection, secure data aggregation and secure routing for WSNs; however, many security challenges are remained exist. The author summarized these challenges and pointed out the following issues:

- Choosing of adequate cryptographic method is relied on the sensor nodes processing capabilities; therefore, there is no combined or unified solution that fit all WSNs.

- As there are many constraints that are related to WSNs such as computation capability, storage, etc.; therefore, any design that is presented for WSNs security services must adequately satisfy these constraints.

- Most of the existing protocols assume the stationary of the sensor nodes. But they are not considered the case if these sensors need to be mobile.

Roman and Lopez [64] analyzed the security issues arise when integrating WSNs to the Internet. They came up with that, the interaction between a sensor network and the internet will be secure when providing the services of the network through a front-end proxy; however, they addressed that there are other challenges need to be solved in case of integrating sensor nodes into the internet infrastructure. In addition, authors added that the complete integration of WSN to internet is remained as an open issue.

This section covers different types of WSNs such as CWSNs, UWSNs, BWSNs, etc. In addition, it has covered most of WSN Attacks mainstream and discussed the proposed countermeasures against them. The achievements and limitations of these proposed solutions are fully stated.

5. CONCLUSION

Security in WSNs is challenging and critical to the functionality of this type of networks. The major challenge is not only to get WSNs secured but is how to get an adequate security system that take into consider the limited resources of such networks and at the same time to keep the system performance integral and intact.

The sole behind the rapid growth of sensors networks is mainly based on its characteristics and performance, therefore any security mechanism that is causing overheads or affecting functionality it doesn't make any sense and thus will not be considered. So again, the major challenge is how to have this balance.

Till now, most of proposed security schemes are based on particular network model. Therefore, a combining effort to represent a common model that take into consideration the security issues concerning each layer still challenge.
The paper concludes and comes out with the following security issues that still need more efforts:

- Cryptography is an adequate security solution for many scenarios of WSNs but still needs more enhancements to reduce the overheads to an acceptable rate that fit WSNs particularities and constraints.

- In terms of security, the integration of WSNs to internet or Internet of Things (IoT) is challenging and critical; therefore, a huge collaboration between designers and security professionals is highly required to bring up an adequate platform that facilities this integration properly and securely.

- The mainstream of WSN security attacks not yet meet the sufficient security solutions.

- Most of proposed security solutions are not effectively considered the WSNs characteristics and its source limitations.

- Mobility on WSNs brings up many challenges to WSNs security.

Commonly, the WSNs security can be enhanced by the rapid development and the advanced technology in designing devices that can deliver high speed, fewer cost value, fewer energy consumption and enable adequate storage space. This is due the fact that the WSN source limitations, constraints,

and particularities are the core problem that weakens most of the proposed security solutions.

Future research could focus on developing a security approach that considers all WSN constraints and particularities and should be driven by the advanced technologies that capable to deal with such constraints. A balance solution is highly needed to satisfy both the WSN security and its constraints.

REFERENCES

1. Z. Ishaq, P. Seongjin, and Y. Younghwan, "A security framework for Cluster-based Wireless Sensor Networks against the selfishness problem," in Ubiquitous and Future Networks (ICUFN), 2015 Seventh International Conference on, 7-10 July 2015 2015, pp. 7-12, doi: 10.1109/ICUFN.2015.7182485.
2. S. Sendra, J. Lloret, M. García, and J. F. Toledo, "Power Saving and Energy Optimization Techniques for Wireless Sensor Neworks," Journal of communications, vol. 6, no. 6, pp. 439-459, 2011. https://doi.org/10.4304/jcm.6.6.439-459
3. F. Xin, D. Xin, and S. Supeng, "A security detection scheme based on evidence nodes in Wireless Sensor Networks," in Biomedical Engineering and Informatics (BMEI), 2013 6th International Conference on, 16-18 Dec. 2013 2013, pp. 689-693, doi: 10.1109/BMEI.2013.6747027.
4. H. Yang, L.-X. Wei, and X.-Y. Yang, "Sybil attack detection scheme in wireless sensor network," Computer Engineering, vol. 12, p. 042, 2011.
5. Harshita Chaurasiya and Shivnath Ghosh, " Performance Evaluation of Energy-Efficient Cluster based Algorithms in Wireless Sensor Network," International Journal of Advanced Trends in Computer Science and Engineering, vol. 7, no. 5, 2018. https://doi.org/10.30534/ijatcse/2018/03752018
6. C. Xiangqian, M. Kia, Y. Kang, and N. Pissinou, "Sensor network security: a survey," Communications Surveys & Tutorials, IEEE, vol. 11, no. 2, pp. 52-73, 2009, doi: 10.1109/SURV.2009.090205.
7. A. K. Pathan, L. Hyung-Woo, and H. Choong Seon, "Security in wireless sensor networks: issues and challenges," in Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, 20-22 Feb. 2006 2006, vol. 2, pp. 6 pp.-1048, doi: 10.1109/ICACT.2006.206151.
8. A. Larsson and P. Tsigas, "Security in Wireless Sensor Networks," in Computer Network Defense (EC2ND), 2011 Seventh European Conference on, 6-7 Sept. 2011 2011, pp. 61-61, doi: 10.1109/EC2ND.2011.13.
9. M. V. M. Sawale and A. S. Kapse, "Enhanced Data Transmission for Cluster-Based Wireless Sensor Networks," 2014.
10. H. Marzi and A. Marzi, "A security model for wireless sensor networks," in Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2014 IEEE International Conference on, 5-7 May 2014 2014, pp. 64-69, doi: 10.1109/CIVEMSA.2014.6841440.
11. D. G. Padmavathi and M. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," arXiv preprint arXiv:0909.0576, 2009.
12. I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1910-1923, 2017. https://doi.org/10.1109/JIOT.2017.2749883
13. E. Shi and A. Perrig, "Designing secure sensor networks," Wireless Communications, IEEE, vol. 11, no. 6, pp. 38-43, 2004, doi: 10.1109/MWC.2004.1368895.
14. T. Kavitha and D. Sridharan, "Security vulnerabilities in wireless sensor networks: A survey," Journal of information Assurance and Security, vol. 5, no. 1, pp. 31-44, 2010.
15. B. K. Mishra, M. C. Nikam, and P. Lakkadwala, "Security against Black Hole Attack in Wireless Sensor Network - A Review," in Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, 7-9 April 2014 2014, pp. 615-620, doi: 10.1109/CSNT.2014.129.
16. S. Misra, K. Bhattarai, and G. Xue, "BAMBi: blackhole attacks mitigation with multiple base stations in wireless sensor networks," in Communications (ICC), 2011 IEEE International Conference on, 2011: IEEE, pp. 1-5.
17. G. Gulhane and N. Mahajan, "Performance Evaluation of Wireless Sensor Network under Black Hole Attack."
18. P. Schaffer, K. Farkas, Á. Horváth, T. Holczer, and L. Buttyán, "Secure and reliable clustering in wireless sensor networks: a critical survey," Computer Networks, vol. 56, no. 11, pp. 2726-2741, 2012.
19. H. Lu, J. Li, and M. Guizani, "Secure and efficient data transmission for cluster-based wireless sensor networks," IEEE transactions on parallel and distributed systems, vol. 25, no. 3, pp. 750-761, 2013. https://doi.org/10.1109/TPDS.2013.43
20. M. Elhoseny, X. Yuan, H. K. El□Minir, and A. M. Riad, "An energy efficient encryption method for secure dynamic WSN," Security and Communication Networks, vol. 9, no. 13, pp. 2024-2031, 2016.
21. M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption," Journal of King Saud University-Computer and Information Sciences, vol. 28, no. 3, pp. 262-275, 2016.
22. T. Khan, K. Singh, M. Abdel-Basset, H. V. Long, S. P. Singh, and M. Manjul, "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks," IEEE Access, vol. 7, pp. 58221-58240, 2019.

23. O. Osanaiye, A. Alfa, and G. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," Sensors, vol. 18, no. 6, p. 1691, 2018.
24. V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Energy Depletion Attacks in Low Power Wireless Networks," IEEE Access, vol. 7, pp. 51915-51932, 2019.
25. N. Geethanjali and E. Gayathri, "A survey on energy depletion attacks in wireless sensor networks," 2012.
26. C. Lin, Z. Shang, W. Du, J. Ren, L. Wang, and G. Wu, "CoDoC: A Novel Attack for Wireless Rechargeable Sensor Networks through Denial of Charge," 2019: IEEE, pp. 856-864.
27. H. Chen, C. Meng, Z. Shan, Z. Fu, and B. K. Bhargava, "A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation," IEEE Access, vol. 7, pp. 32853-32866, 2019.
28. M. Jamshidi, E. Zangeneh, M. Esnaashari, A. M. Darwesh, and M. R. Meybodi, "A Novel Model of Sybil Attack in Cluster-Based Wireless Sensor Networks and Propose a Distributed Algorithm to Defend It," Wireless Personal Communications, vol. 105, no. 1, pp. 145-173, 2019.
29. S. Chen, G. Yang, and S. Chen, "A security routing mechanism against Sybil attack for wireless sensor networks," 2010, vol. 1: IEEE, pp. 142-146. https://doi.org/10.1109/CMC.2010.265
30. D. Kukreja, M. Miglani, S. K. Dhurandher, and B. V. R. Reddy, "Security enhancement by detection and penalization of malicious nodes in wireless networks," in Signal Processing and Integrated Networks (SPIN), 2014 International Conference on, 20-21 Feb. 2014 2014, pp. 275-280, doi: 10.1109/SPIN.2014.6776962.
31. X. Yuanpeng et al., "The security issue of WSNs based on cloud computing," in Communications and Network Security (CNS), 2013 IEEE Conference on, 14-16 Oct. 2013 2013, pp. 383-384, doi: 10.1109/CNS.2013.6682739.
32. G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," Sensors, vol. 18, no. 11, p. 3907, 2018.
33. X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Secure and efficient time synchronization in heterogeneous sensor networks," IEEE transactions on vehicular technology, vol. 57, no. 4, pp. 2387-2394, 2008. https://doi.org/10.1109/TVT.2007.912327
34. A. Boukerche and D. Turgut, "Secure time synchronization protocols for wireless sensor networks," IEEE Wireless Communications, vol. 14, no. 5, pp. 64-69, 2007. https://doi.org/10.1109/MWC.2007.4396944
35. H. Song, S. Zhu, and G. Cao, "Attack-resilient time synchronization for wireless sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 112-125, 2007.
36. N. Tuptuk and S. Hailes, "Covert channel attacks in pervasive computing," 2015: IEEE, pp. 236-242.
37. M. A. Elsadig and Y. A. Fadlalla, "Packet Length Covert Channel: A Detection Scheme," 2018: IEEE, pp. 1-7.
38. M. A. Elsadig and Y. A. Fadlalla, "Packet Length Covert Channels Crashed." Journal of Computer Science & Computational Mathematics (JCSCM), vol. 8, no. 4, pp. 55-62, 2018.
39. A. Swaminathan and P. Vivekanandan, "Probablistic Queuing Model to Detect Covert Channel Communication in Wireless Sensor Network."
40. M. A. Elsadig and Y. A. Fadlalla, "Network Protocol Covert Channels: Countermeasures Techniques," 2017: IEEE, pp. 1-9.
41. M. A. Elsadig and Y. A. Fadlalla, "An Efficient Approach to Resolve Covert Channels," IJ Network Security, vol. 20, no. 5, pp. 898-906, 2018.
42. M. A. Elsadig, "Resolving Network Packet Length Covert Channels," Diss. Sudan University of Science & Technology, 2018.
43. M. Valero, S. Uluagac, S. Venkatachalam, K. C. Ramalingam, and R. Beyah, "The Monitoring Core: A framework for sensor security application development," in Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on, 8-11 Oct. 2012 2012, pp. 263-271, doi: 10.1109/MASS.2012.6502525.
44. Z. Yanmin, K. Sye Loong, M. Sloman, E. Lupu, N. Dulay, and N. Pryce, "A policy system to support adaptability and security on body sensors," in Medical Devices and Biosensors, 2008. ISSS-MDBS 2008. 5th International Summer School and Symposium on, 1-3 June 2008 2008, pp. 37-40, doi: 10.1109/ISSMDBS.2008.4575010.
45. A. S. Sangari and J. M. L. Manickam, "Public key cryptosystem based security in wireless body area network," 2014: IEEE, pp. 1609-1612.
46. J. Shen, W.-Y. Zheng, J. Wang, Y.-H. Zheng, X.-M. Sun, and S.-Y. Lee, "An efficient verifiably encrypted signature from weil pairing,", vol. 14, no. 6, pp. 947-952, 2013.
47. C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: a lightweight identity-based cryptography for body sensor networks," IEEE Transactions on Information Technology in Biomedicine, vol. 13, no. 6, pp. 926-932, 2009.
48. J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," IEEE Transactions on computers, vol. 64, no. 2, pp. 425-437, 2013.
49. J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," Future generation computer systems, vol. 78, pp. 956-963, 2018.
50. T. Hayajneh, G. Almashaqbeh, S. Ullah, and A. V. Vasilakos, "A survey of wireless technologies coexistence in WBAN: analysis and open research issues," Wireless Networks, vol. 20, no. 8, pp. 2165-2199, 2014.

51. Y. Qu, G. Zheng, H. Ma, X. Wang, B. Ji, and H. Wu, "A Survey of Routing Protocols in WBAN for Healthcare Applications," Sensors, vol. 19, no. 7, p. 1638, 2019.
52. J. Kang and S. Adibi, "A review of security protocols in mHealth wireless body area networks (WBAN)," 2015: Springer, pp. 61-83.
53. K.Vallimadhavi, P Sivaprasad, R.Baladinakar, Y.D.Siva Prasad, and K.D.S.Naidu, "Automatic connection of various medical sensors by using WBAN adaptive routing protocol," International Journal of Advanced Trends in Computer Science and Engineering, vol. 6, no. 7, 2018
https://doi.org/10.30534/ijatcse/2018/14762018
54. P. Uppuluri and S. Basu, "LASE: Layered approach for sensor security and efficiency," in Parallel Processing Workshops, 2004. ICPP 2004 Workshops. Proceedings. 2004 International Conference on, 18-18 Aug. 2004 2004, pp. 346-352, doi: 10.1109/ICPPW.2004.1328038.
55. C. Haiguang, W. Huafeng, Z. Xi, and G. Chuanshan, "Agent-based Trust Model in Wireless Sensor Networks," in Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on, July 30 2007-Aug. 1 2007 2007, vol. 3, pp. 119-124, doi: 10.1109/SNPD.2007.122.
56. Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," Computers & Security, vol. 39, pp. 351-365, 2013.
57. O. Khalid et al., "Comparative study of trust and reputation systems for wireless sensor networks," Security and Communication Networks, vol. 6, no. 6, pp. 669-688, 2013.
58. R. Gupta, K. Sultania, P. Singh, and A. Gupta, "Security for wireless sensor networks in military operations," in Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on, 4-6 July 2013 2013, pp. 1-6, doi: 10.1109/ICCCNT.2013.6726654.
59. S. S. Desai and M. J. Nene, "Node-level trust evaluation in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 2139-2152, 2019.
60. G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public key cryptography in sensor networks—revisited," 2004: Springer, pp. 2-18.
61. M. Saleh and I. Al Khatib, "Throughput analysis of WEP security in ad hoc sensor networks," in Proc. The Second International Conference on Innovations in Information Technology (IIT'05), September, 2005, pp. 26-28.
62. G. Panic, T. Basmer, and O. Schrape, "A power-gated sensor node microcontroller for security applications," in Radio Science Conference (URSI AT-RASC), 2015 1st URSI Atlantic, 16-24 May 2015 2015, pp. 1-1, doi: 10.1109/URSI-AT-RASC.2015.7302980.
63. J. Sen, "A survey on wireless sensor network security," arXiv preprint arXiv:1011.1529, 2010.
64. R. Roman and J. Lopez, "Integrating wireless sensor networks and the internet: a security analysis," Internet Research, vol. 19, no. 2, pp. 246-259, 2009, doi: doi:10.1108/10662240910952373.