THE CHALLENGES AND VIABILITY OF USING BLOCKCHAIN FOR WSN SECURITY

Muhammad R. Ahmed, Thirein Myo and Badar Al Baroomi

Military Technological College, Muscat, Oman

ABSTRACT

Wireless Sensor Network (WSN) comprises of cheap and multifunctional resources constrain nodes that communicate at a fair distances through wireless connections. It is open media and underpinned by an application scenario for data collecting and processing. It can be used for many exclusive applications range from military implementation inside the battlefield, environmental tracking, fitness quarter as well as emergency response of surveillance. With its nature and application scenario, protection of WSN had drawn an attention. It is understood that the sensor nodes are valuable to the attacks because of the construction nature of the sensor nodes and distributed network infrastructure. In order to ensure its capability especially in malicious environments, security mechanisms are essential. In this paper, we have discussed the challenges and the viability of the blockchain to implement in the WSN in order to protect WSN from the attacks.

KEYWORDS

Wireless Sensor Network, Security, challenges, blockchain.

1. INTRODUCTION

Wireless sensor networks (WSNs) and their applications are becoming part of our daily life, they have a great advantage for various applications in our real life [1], such as habitat monitoring, battlefield surveillance, intelligent agriculture, home automation, etc. However, the properties of WSN inevitably have the natures that are extremely restricted by their resources, including energy, memory, computing complexity, bandwidth, and communication capacity. Normally the base station is a more powerful node, which can be linked to a central station via satellite or internet communication to form a network. There are many deployments for wireless sensor networks depending on various applications, such as, environmental monitoring, volcano detection [1-3], distributed control systems [4], agricultural and farm management [5], detection of radioactive sources [6], and computing platform for tomorrows' internet [7]. However, the open nature of the wireless medium therefore offers chances for an adversary to easily eavesdrop information from the sensors, or actively do something such as replay or inject fabricated messages. A Typical WSN is shown in Figure 1.

In all communication network including WSN, Security provisioning is a critical requirement. Security in the wireless sensor network is challenging and important task because of its characteristics that includes, open nature of wireless medium, unattended operation, limited energy, memory, computing power, communication bandwidth, and communication range. So, it is more susceptible to the security attack compared to the traditional wired network. It is well known that for the protection from the some WSNs attacks, various cryptographic methods are widely used but sometimes are not very efficient and effective [8-9].

David C. Wyld et al. (Eds): CCNET, NLTM, CICS - 2022
pp. 11-18, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.120302

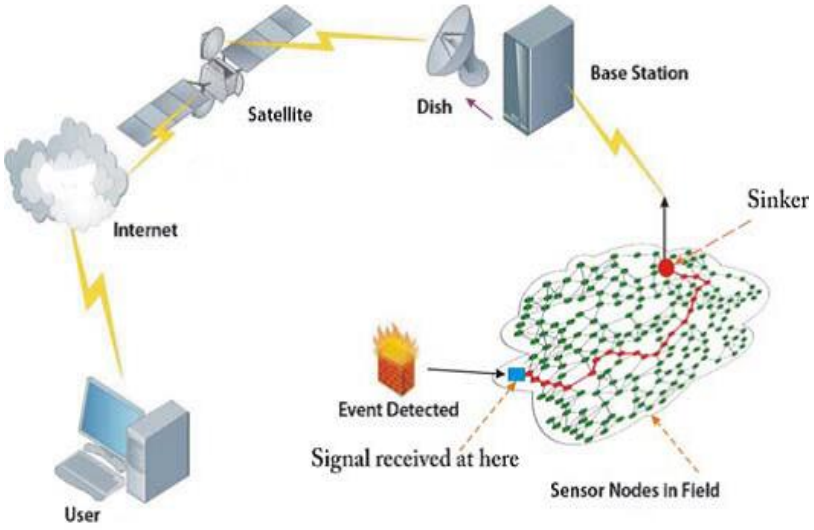

Figure 1. A typical WSN [1]

Blockchain is a method that lets the transmission of data securely based on an incredibly complex encryption mechanism. In this mechanism, each block includes records about its advent time and is related to the previous block by using hash code and transaction information. When the data is recorded in the blockchain, there's almost impossible to change it [10]. Blockchain is designed to resist fraud and alteration of facts. Implement blockchain into WSNs will deliver few advantages:[11]

a. The distributed nature of blockchain will allow a large number of sensor node connection easily
b. Computing and storage needs are distributed to all devices in the network, this will reduce the cost of the large central data
c. Centralized Server and Client Model will be eliminated when peer-to-peer messaging, file distribution, and automatic coordination between devices in the network are used

In this paper, we are focusing on investigating the possible viability and major challenges to implement the blockchain to secure WSN.

This paper consists of five sections. A brief discussion of the characteristics of WSN is in Section II. Section III describes the architecture of WSN. Section IV describes the blockchain structure. A brief discussions of WSN security with blockchain is given in Section V. conclusion is in Section VI

2. CHARACTERISTICS OF WSN

WSN is currently used for real-world unattended physical environment to measure numerous parameters. So, the characteristics of WSN must be considered for efficient deployment of the network. The significant characteristics of WSN are described as follows [12]:

Low cost: in the WSN normally hundreds or thousands of sensor nodes are deployed to measure any physical environment. To reduce the overall cost of the whole network, the cost of the sensor node must be kept as low as possible.

Energy efficient: energy in WSN is used for different purpose such as computation, communication, and storage. Sensor node consumes more energy compared to any other for communication. If they run out of power, they often become invalid as we do not have any option to recharge. So, the protocols and algorithm development should consider the power consumption in the design phase.

Computational power: normally node has limited computational capabilities as the cost and energy need to be considered.

Communication Capabilities: WSN typically communicate using radiowaves over a wireless channel. It has the property of communicating in short range, with narrow and dynamic bandwidth. The communication channel can be either bidirectional or unidirectional. With the unattended and hostile operational environment, it is difficult to run WSN smoothly. So, the hardware and software for communication must have to consider the robustness, security, and resiliency.

Security and Privacy: Each sensor node should have sufficient security mechanisms to prevent unauthorized access, attacks, and unintentional damage of the information inside of the sensor node. Furthermore, additional privacy mechanisms must also be included.

Distributed sensing and processing: the large number of sensor node is distributed uniformly or randomly. WSNs each node can collect, sort, process, aggregate and send the data to the sink. Therefore, the distributed sensing provides the robustness of the system.

Dynamic network topology: in general, WSN a dynamic network. The sensor node can fail for battery exhaustion or other circumstances, communication channel can be disrupted as well as the additional sensor node may be added to the network that result the frequent changes in the network topology. Thus, the WSN nodes must be embedded with the function of reconfiguration, self-adjustment.

Self-organization: the sensor nodes in the network must have the capability of organizing themselves as the sensor nodes are deployed in an unknown fashion in an unattended and hostile environment. The sensor nodes have work in collaboration to adjust themselves to the distributed algorithm and form the network automatically.

Multi-hop communication: a large number of sensor nodes are deployed in WSN. So, the feasible way to communicate with the sinker or base station is to take the help of an intermediate node through routing path. If one need to communicate with the other node or base station which is beyond its radio frequency it must be through the multi-hop route by intermediate node.

Application oriented: WSN is different from the conventional network due to its nature. It is highly dependent on the application ranges from military, environmental as well as health sector. The nodes are deployed randomly and spanned depending on the type of use.

Robust Operations: Since the sensors are going to be deployed over a large and sometimes hostile environment. So, the sensor nodes must be fault and error tolerant. Therefore, sensor nodes need the ability to self-test, self-calibrate, and self-repair.

Small physical size: sensor nodes are generally small with the restricted range. Due to its size its energy is limited which makes the communication capability low.

3. ARCHITECTURE OF WSN

WSN is dynamic which can consist of various types of sensor nodes. The environment is heterogeneous in terms of both hardware as well as software. The sensor node construction focuses to reduce cost, increase flexibility, provide fault tolerance. Improve development process and conserve energy. The structure of sensor node consists of sensing unit (sensor and analog to digital converter), processing unit (processor and storage), communication unit (transceiver), and power supply unit. [13] The major blocks shown in Figure 2. A concise description of different unit is as follows [13-17]:

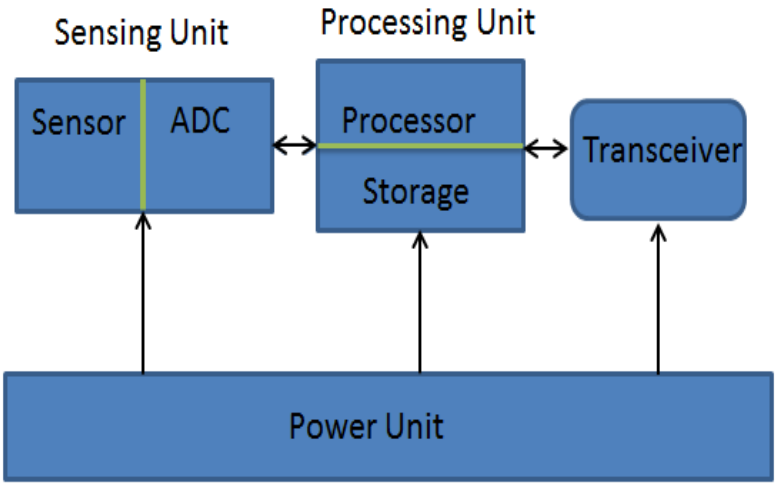

Figure 2. Structure of a sensor node

Sensing unit: it is composed of collection of different types of sensors which is needed for measurement of different phenomenon of the physical environment. Sensors are selected based on its application. Sensor out is electric signal which is analog. So, analog-to-digital converter (ADC) is used to transform the signal to digital in order to communicate with the microcontroller.

Processing unit: it consists of a processor (microcontroller) and storage (RAM). In addition, it has operating systems as well as timer. The responsibility of the processing unit includes collecting data from various sources than processing and storing. Timer is used to do the sequencing for the sequence.

Communication unit: it uses a transceiver which consists of a transmitter as well as a receiver. The communication is performed through the communication channels by using the network protocol. Based on the application requirements and relevance to communicate it normally uses suitable method such as radio, infrared or optical communication.

Power unit: the task of the power unit is to provide the energy to the sensor node for monitoring the environment at a low cost and less time. The life of the sensor depends on the battery or power generator which is connected to the power unit. Power unit is required for the efficient use of the battery.

WSN communication architecture is a bit different from the conventional computer communication and computer network. The communication architecture can be classified in different layers. To get the maximum efficiency with limited resources and low overhead WSN does not adhere as closely to the layered architecture of OSI model of conventional network.

Nevertheless, the layered model is useful in WSN for categorizing protocols, attacks and defence. So, in contrast to the traditional seven layers it is reduced to the five layers [13] that include physical layer, Data link layer, network layer, transport layer and application later. The advantage of the layered model is conceptually similar functions are combined at one layer. Figure 3 shows the communication protocol model of wireless sensor network.

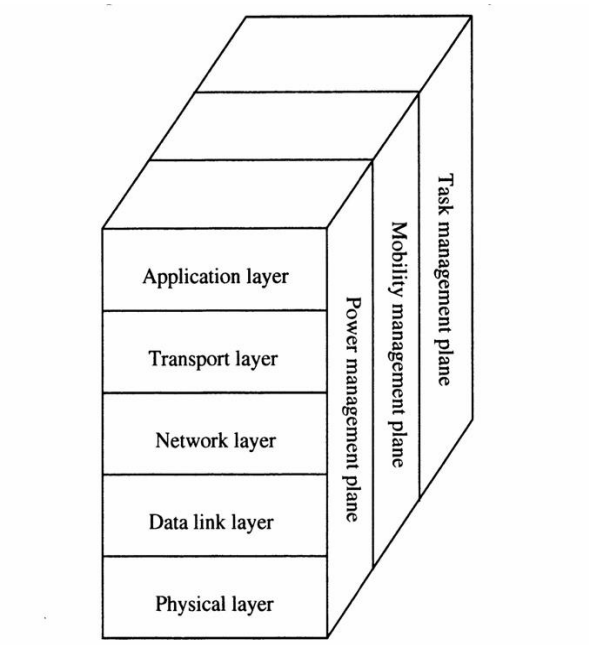

Figure 3. Protocol Stack of WSN [13]

The physical layer addresses the hardware detail of wireless communication mechanism. This layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. The data link layer is concerned with the media access control (MAC) protocol. Since the wireless channel is susceptible to the noise and sensor nodes may be changing the location MAC protocol at the data link layer has to be power-aware and should have the capability of minimizing the collisions.[4] The network layer manages the routing the data supplied by the transport layer or between the nodes. Whereas the transport layer can maintain the data flow if the WSN application requires that. Various type of application can be implemented in the application depending on the physical environmental sensing.

Orthogonal to the five-layer Akyildiz et al. [13] defined three management plan named power, mobility and task management. These plans are responsible for monitoring the power, movement and task distribution among the sensor nodes. These management plans help the sensor nodes to coordinate sensor tasks and minimize the overall power consumption font.

4. BLOCKCHAIN STRUCTURE

Blockchain technology allow untrusting parties with common interests to exchange the information without relying on the external entities. Core characteristics of blockchain is decentralization, accountability, and security. This technique can improve operational efficiency and save costs of the network significantly. In order to achieve the decentralization blockchain, it uses the peer-to-peer (P2P) network architecture [18]. Early blockchain technology based on P2P networking has improved the decentralized network architecture. Figure 4 shows decentralized blockchain. it consists of three important concepts [19]:

1. Blocks,
2. Nodes and
3. Miners.

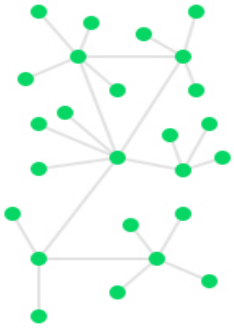

Figure 4. Decentralized Blockchain

Blocks: Each chain consists of several blocks and each block has information data, a nonce and the hash. Whenever the primary block of a chain is formed, a nonce then creates the cryptographic hash. The information data within the block is considered signed and for all time tied to the nonce and hash except it's far mined.

Nodes: Every node has its specific copy of the blockchain and the network have to algorithmically approve any newly excavated block for the chain to be up to date, trusted and verified. Since blockchains are transparent, so it is easy to check and verify each action and record within the ledger. Each node is given a unique number that shows their transactions.

Miners: Miners normally use specific program to solve the extremely complex mathematical problem of finding a nonce that generates hash which can be accepted.

5. DISCUSSIONS OF WSN SECURITY WITH BLOCKCHAIN

The security provisioning in WSN is a critical task. Several works has been done by researchers to secure the WSN. Recently, the focus was given to blockchain for the data security, management and storage of WSN. Moinet et al. proposed a blockchain based multi sensor technique [20]. This technique collects and verify the information data gathered by the sensor. Casado vara et al. proposed stochastic model of blockchain [21]. This can do the early prediction of the degeneration of the sensor accuracy from the current state of the sensor. Cui et al. proposed a hybrid blockchain model [22]. This method, realize the authentication from different communication scenarios. The previous studies mentioned have several constraints. Moreover, they did not consider the decentralized model of blockchain. A Comparison is drawn in the Table 1. To compare the WSN with the blockchain implementation and without the blockchain.

Table 1. WSN with and without Blockchain

Attributes	Without Blockchain	With Blockchain
Architecture	It is centralised with client-server architecture	Based on the distributed ledger architecture with decentralization
Power consumption	Low	High
Security	Low	High
Device Requirements	It requires limited processing capability with low storage capacity	It requires high processing capability with high storage capacity
Implementation	Simple	Difficult
Maintenance	Easy	Difficult

Considering the current architecture of WSN, sensor nodes are normally with the low capacity, low possessing power, limited storage, and limited battery capacity. Blockchain technology will bring a new arena of the WSN security as it has decentralised capacity and it can give better security. To implement Blockchain in WSN it requires high configuration sensors with high processing capability and high storage and high battery support. Moreover, WSN with the blockchain is difficult to implement and maintain. As a result, there are few challenges to implement blockchain for WSN security. Blockchain distributed character will be lost if the WSN need to be extended. So WSN will loss the scalability. Current sensor nodes do not have the high power and processing time. So, implementing Blockchain with current sensors will face difficulties with the processing speed and battery power. Blockchain requires to store transection and device ID. So, it requires high storage. Moreover, implement and maintain blockchain need highly skilled professionals.

It is difficult to implement blockchain in current resource constrain WSN, the technology requires huge resources. In order to incorporate blockchain in WSN and make it reality, we need to look forward for advancement of microelectronics to make the sensors resourceful. As the microelectronics is evolving very fast, so the blockchain soon will become the reality for WSN security . With the current infrastructure of WSN, blockchain is possible to implement but it will not be able to support the voice and video data because of storage and battery life of the sensor node.

6. CONCLUSION

Currently, the implementation of blockchain in WSN is challenging task as blockchain is still in early stage in implementing in engineering applications. The main challenge is the requirement of higher memory in each node in the network with blockchain as it does not use central server. The distributed the nature of blockchain require high memory and hardware in each node. However, it is believed that the current trend of advancement in memory technology will provide the high memory capacity with very small size in very near future. Some of the research is showing promising result which can fulfil this requirement. However, the distributed and secure architecture of blockchain will fulfil the challenges currently facing in WSN network. In future, we would like to implement blockchain for WSN security utilizing the text data transmission.

REFERENCES

[1] X. Huang, M. Ahmed, and D. Sharma, “Timing control for protecting from internal attacks in wireless sensor networks,” in 2012 International Conference on Information Networking (ICOIN), 2012, pp. 7 –12.

[2] D. Li, K. D. Wong, Y. H. Hu, and A. M. Sayeed, “Detection, classification, and tracking of targets,” IEEE Signal Processing Magazine, vol. 19, no. 2, pp. 17 –29, Mar. 2002.

[3] C. Meesookho, S. Narayanan, and C. S. Raghavendra, “Collaborative classification applications in sensor networks,” in Sensor Array and Multichannel Signal Processing Workshop Proceedings, 2002, 2002, pp. 370 – 374.
[4] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui, and B. Krogh, “Energy-efficient surveillance system using wireless sensor networks,” in Proceedings of the 2nd international conference on Mobile systems, applications, and services, New York, NY, USA, 2004, pp. 270–283.
[5] B. Sinopoli, C. Sharp, L. Schenato, S. Schaffert, and S. S. Sastry, “Distributed control applications within sensor networks,” Proceedings of the IEEE, vol. 91, no. 8, pp. 1235 – 1246, Aug. 2003.
[6] P. Sikka, P. Corke, P. Valencia, C. Crossman, D. Swain, and G. Bishop-Hurley, “Wireless ad hoc sensor and actuator networks on the farm,” in The Fifth International Conference on Information Processing in Sensor Networks, 2006. IPSN 2006, 2006, pp. 492 –499.
[7] F. Zhao, “Wireless sensor networks: a new computing platform for tomorrow’s Internet,” in Proceedings of the IEEE 6th Circuits and Systems Symposium on Emerging Technologies: Frontiers of Mobile and Wireless Communication, 2004, May-2 June, vol. 1, pp. I–27 Vol.1.
[8] M. Ahmed, X. Huang, and D. Sharma, “A Taxonomy of Internal Attacks in Wireless Sensor Network,” in World Academy of Science, Engineering and Technology, Kuala Lumpur, Malaysia, 2012, pp. 427–430.
[9] M. Ahmed, X. Huang, and D. Sharma, “A Novel Framework for Abnormal Behaviour Identification and Detection for Wireless Sensor Networks,” International Journal of Computer and Communication Engineering, vol. 6, no. 2, pp. 148–151, 2012.
[10] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues”, Telematics and Informatics, Volume 36, 2019, Pages 55-81, ISSN 0736-5853
[11] David Berdik, Safa Otoum, Nikolas Schmidt, Dylan Porter, Yaser Jararweh, “A Survey on Blockchain for Information Systems Management and Security, “Information Processing & Management, Volume 58, Issue 1, 2021, 102397, ISSN 0306-4573
[12] Ahmed, M. , Huang, X. , Sharma, D. , Cui, H. (2012), 'Wireless Sensor Network: Characteristics and Architectures', World Academy of Science, Engineering and Technology, Open Science Index 72, International Journal of Information and Communication Engineering, 6(12), 1398 - 1401.
[13] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E, Cayirci, “A Survey on Sensor Networks”, IEEE Communications Magazine , August 2002.
[14] H. Karl, A, Willing, “Protocols and Architectures for Wireless Sensor Networks”. New York: Wiley, 2005. 314−340, 2005.
[15] C. Buratti , A. Conti , D. Dardari and R, Verdone, “An Overview on Wireless Sensor Networks Technology and Evolution” , Sensors 2009, ISSN 1424-8220, pp 6869-6896, 2009.
[16] K. v. madhav , C ,rajendra and R. L. selvaraj, “A study of security challenges in wireless sensor networks”, Journal of Theoretical and Applied Information Technology, 2010.
[17] J. Feng, F. Koushanfar, and M. Potkonjak, ” Sensor Network Architecture”, supported by the national science foundation under Grant No. NI-0085773 and NSF CENS Grant, 2005.
[18] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.
[19] Wu, J.; Tran, N.K. Application of Blockchain Technology in Sustainable Energy Systems: An Overview. Sustainability 2018, 10, 3067. https://doi.org/10.3390/su10093067.
[20] Moinet, A., Darties, B., & Baril, J. L. (2017). Blockchain based trust & authentication for decentralized sensor networks. arXiv preprint arXiv:1706.01730.
[21] Casado-Vara, R. (2018, June). Stochastic approach for prediction of WSN accuracy degradation with blockchain technology. In International Symposium on Distributed Computing and Artificial Intelligence (pp. 422-425). Springer, Cham.
[22] Cui, Z., Fei, X. U. E., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybridBlockChain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing, 13(2), 241-251.