Chapter

Challenges of WSNs in IoT

Brijesh Kundaliya

Abstract

IoT and WSNs are the prime moving force for technology in the current world. WSNs unfold their capacity day by day in almost every aspect of life. IoT enables to integrate the different devices and makes it possible to communicate with each other. It makes life easier and upgrades the application's usage to the next level. The integration of WSNs with IoT will help to reach apical of the usage of applications. The combination of WSNs and IoT will open up new doors in almost all the possible fields however the amalgamation of both the technology needs careful consideration about bringing the both on same level. The IoT is considered a mighty giant with enormous power and capability. On the other side, WSNs are miniature having limited resources but the tremendous capability to penetrate in almost every aspect of life. WSN's limited resources are the main concern while integrating it with the IoT. The integration will make it possible to access the sensor node from any part of the world. It implies that now the sensor node is open for any heterogeneous internet user in the world. It will cause a security issue. Moreover, the topology and addressing of WSNs are different from the normal internet which needs to be addressed during the integrations. And there are other challenges too which we discussed in depth in this chapter.

Keywords: WSNs, IoT, integration, security, addressing

1. Introduction

Wireless Sensor Networks (WSNs) will be the dominating field in the future era. Right now it is in the transformation phase [1]. It unfolds its capacity and is sorting out its limitations. CISCO is a giant player in the networking field. According to CISCO, the number of devices connected to the internet will be around 50 billion by 2021 which is shown in **Figure 1**. We will be surrounded by the sensors, rather on a lighter note, we can say that we will be captured by the sensors. The sensor networks will generate more than 500 zettabytes of data, which may be structured or unstructured data (Cisco Press release, 2018). The WSNs market was valued at USD 46.76 billion and expected that it will reach USD 123.93 by 2025 as depicted in **Figure 2**. The application range of the wireless sensor network is broad, from simple house automation to emergency response robots for forest fire detection.

The number of devices connected with the internet creates the network of the device which enables the controlling of a physical quantity (i.e. room temperature, fan speed, etc. ...) remotely through the internet. This is nothing but the IoT. WSNs and IoT go hand to hand with small differences. So let's first understand the relationship between IoT and the WSNs. If we consider the tree as IoT then the leaf of the tree is the WSNs. WSNs architecture consist of sensor nodes and a sink node as shown in **Figure 3**. The sensor node has to perform two operations: sensing the physical quantity and forward the sensed data. In other words, it has to play two

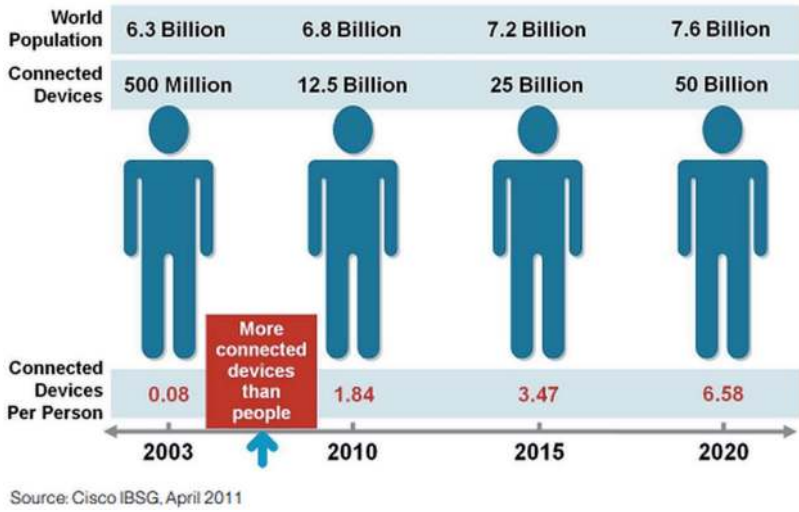

Figure 1.
Number of devices connected to internet (Cisco Press release) [2].

Figure 2.
Market growths of WSNs (ETNO) [2].

roles, as data generating and data forwarding. IoT works at a higher level, which integrate WSNs, any physical object connected to the internet, Internet, Apps, cloud computing, etc. as shown in **Figure 4**. We can say that WSNs can be considered as the subpart of the WSNs as shown in **Figure 5**.

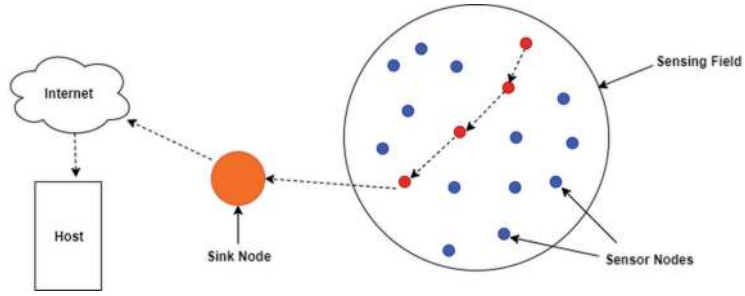

Figure 3.
WSNs architecture.

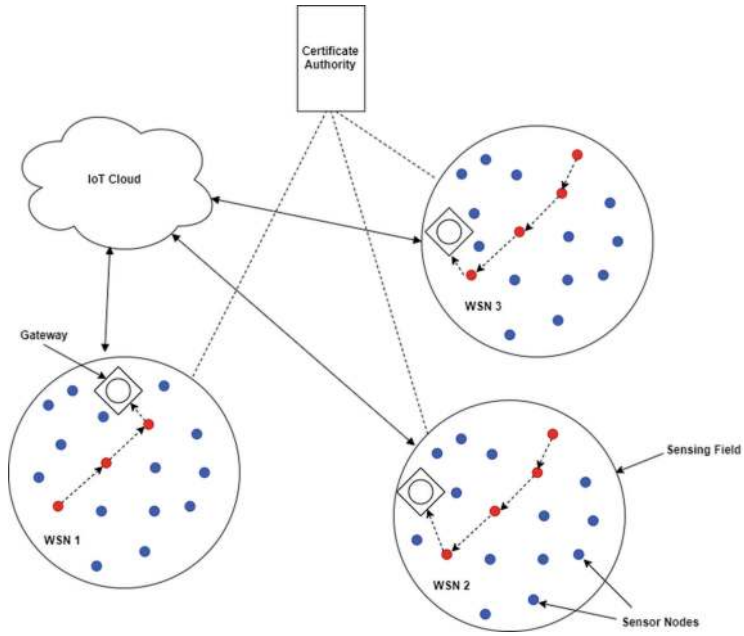

Figure 4.
IoT architecture.

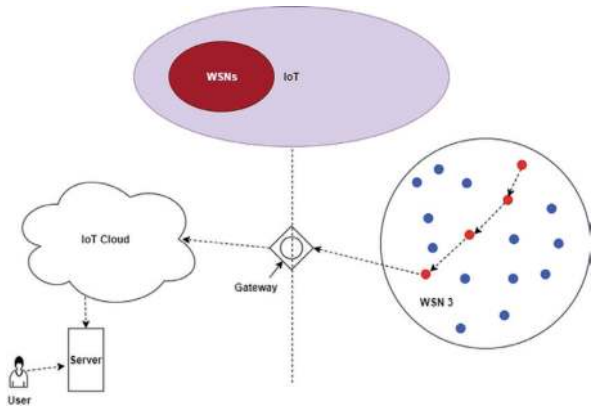

Figure 5.
Interrelation between IoT and WSNs.

2. Integrations and challenges

The integration of the WSNs with the IoT opens the ajar door of applications in every aspect of life. We are aware that in WSNs, the sensor comes with limited capacity in terms of memory, processor, and power, whereas IoT is equipped with abundant resources. It is very much important that the merging of WSNs with the IoT has to be done in a way that they maintain their authentic functions while helping each other to enrich the application ranges [3]. There are certain issues with this integration that is discussed in the following section.

2.1 Connectivity and infrastructure

The first step for integration is the connection of WSNs with the internet. There are three different way by which WSNs is connected with the internet [4]. The first approach is the Front-end proxy solution, in which the base station works as the interface between the sensor nodes and the internet. The base station is the main controlling element that can gather the information from the sensor node or can send any control information to sensor nodes. The base station worked as an insulator between the sensor node and the internet. The Sensor node is completely autonomous that gives the privilege to implements its algorithms and protocol. As shown in the **Figure 6** it is the base station responsibility to map the data of sensor node to equivalent internet protocol and vice versa. Base station has the capability to handle data coming from the internet having TCP/IP compatibility as well as data coming from the sensor node having the format of special sensor network protocol. It also has the capability to communicate with MAC layer as well as IEEE 802.15.4 (wireless standard) [5].

The second approach is the gate-way solution, where a base station serves as the application layer gateway. Here the Base station commands the lower layers of the internet as well as the WSNs. In this approach, WSNs can maintain their individuality at a certain level but still, it is compulsory to create the table, which maps sensor node address to IP address. As we can see in **Figure 7** at base station, sensor data can maintain its individuality up to TCP/IP layer only. At above layer data will be treated as common one.

The third solution is the TCP-IP overlay solution, where the sensor node can directly communicate with the internet using TCP-IP protocol. The base station is worked as a router that connects the two networks. In this approach, the node must need to implement the algorithm and protocol used in the internets. It offers the holistic integration of the WSNs with the internet. It is very much clear form the **Figure 8** that, sensor node must have installed TCP/IP protocol. In this solution, up

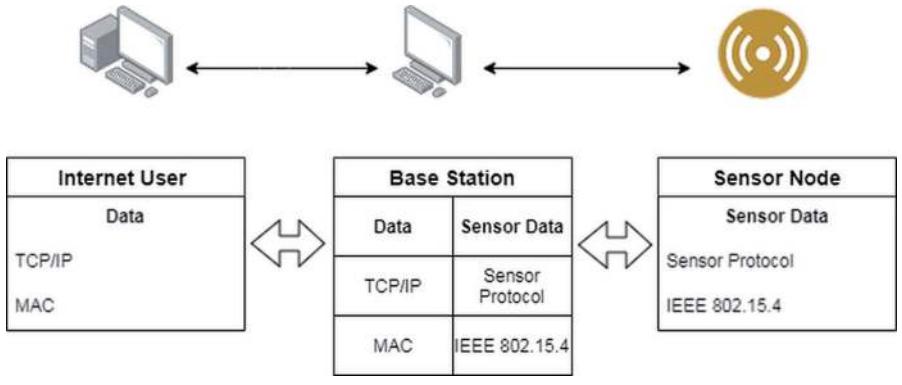

Figure 6.
Front end proxy solution.

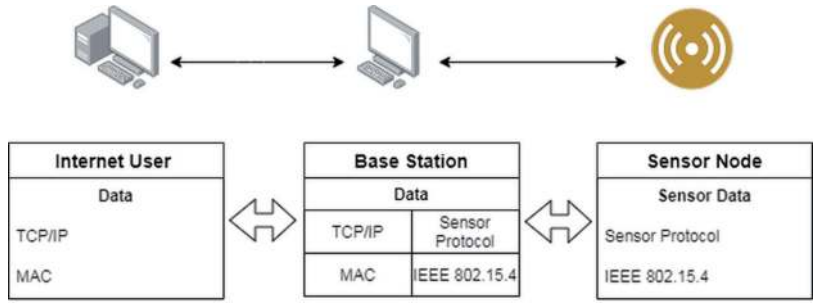

Figure 7.
Gateway solution.

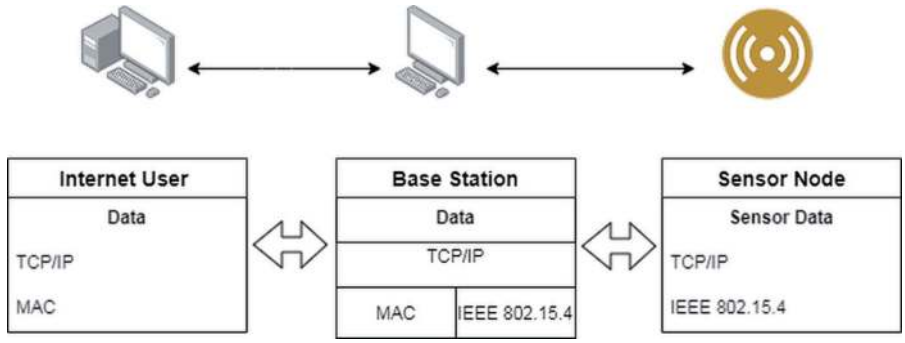

Figure 8.
TCP/IP overlay solution.

to MAC layer the WSNs can maintain its uniqueness after that there is no difference between WSNs data and IoT data.

When we connect the sensor nodes to the internet it certainly enhances the application range and quality. But it is still not clear that up to which extent we need to allow that integration. If we keep the sensor node isolated from the internet that narrows down the capacity of IoT and WSNs. On the other hand, if we go for full integration it is quite difficult for the sensor node to handle the communication with limited resources. There are certain aspects that need to be answered for full integration.

2.2 Addressing

In a front-end proxy solution, the base station needs to have the capability to enable interoperability between WSNs and the Internet. In the second case, the base station has to perform the task of an application layer gateway. It needs to be compatible with internet protocol as well as the WSNs protocol. In the third approach where the node can directly connect with the internet, means the sensor node needs to have direct IP addresses. It is indeed difficult to run standard internet protocol on to the sensor node having limited resources due to following reasons.

i. Deployment: In internet devices are consider as fixed entity. Their physical location remains unchanged throughout the operation. Network administrator is well aware about the topology which is normally remaining fixed. In WSNs the sensor node deployed in the random manner in sensing field. Moreover, in many applications mobile sensor nodes are used. It implies that topology of sensor node are continuously changing.

ii. Vulnerability: Sensors are placed in the event prone area. It is possible that during the operation it might get damage due to any reason and leads to dead node. Moreover, excessive events results in excessive communication that causes excessive energy consumption at the node.

iii. Limited Resources: Sensor node has a limited energy. To enhance the energy utilization it continually changes its states from active mode to sleep mode and vice versa. In sleep mode the sensor node is virtually out of the network which directly affects it topology.

It is very much clear that the addressing of WSNs and IoT is quite different. It is niche factor that decide the faithful operation of the WSNs and IoT's integration. It is utter most important to keep an eye on the topology change of WSNs [6–8].

2.3 Protocols

WSNs is designed for specific applications. Its protocols are tailored according to the specific requirements of the application and surrounding of the event area. Protocols are designed in such a way that it uses minimum information from the network to complete the task. The limited processing capacity and the energy of the node are the reason behind this. On the other side the IoT have the unlimited processing capacity and able to spend more energy in the communication. IoT deals with more broad aspect of applications and hence its protocol must be designed in such a way that it addresses the general aspects [9]. Integrating application specific protocol with the general protocol needs careful approach so that it maintains their endemic operation as well as the interoperability [1, 10].

2.4 Node and data availability

The core focus of WSNs is sensory data. It depends on the availability of the sensor node. WSNs are equipped with fewer resources especially power. To reduce the power usage, the node continuously switches to sleep mode from the active node and vice versa. In the worst situation, due to excessive usage of power node becomes dead. It implies that a particular part of the network is out of range. The sleeping node and dead node are not able to send the data and out of the topology. While we integrating the WSNs with the internet, the external host may not able to collect the data from the node due to the unavailability of the node. In addition to that, a malicious external host can attack a node in several ways i.e. generating the false or dummy data and saturate the node resources like a battery. So it is inevitable to devise a way that can assure the availability node and data correctly.

The mobility of the node in the sensor network is also an essential issue to be dealt with carefully. In many applications, the sensor nodes are continuously changing its position to collect the data. Moreover, WSNs also comes with a new data collecting approach called the mobile sink node. In that, the sink node travels through the network on a specified path to collect the data from the sensor nodes. Here the topology is continuously changed with the time which needs to be handling precisely while integrating with the internet [11].

2.5 Hardware and technological issue

A wireless sensor network is meant for specific applications. The sensor node has to provide specific data for as long as possible time with minimum resources. They use the low data rate communication to save the energy of the nodes. Moreover, the

hardware is design to switch into active and sleep mode. The application for which it is going to be used and the protocol which is going to be implemented, they both need to consider this point during the integration.

WSNs use Tiny OS as the operating system. Tiny OS is the event driven programming model instead of multithreading operation. On same platform other OS like LiteOS, Contiki and 6LoWPAN had be newly developed for WSNs. These OS designed in such a way that it enables the sensor node as and when an event occurs. During other time, sensor node remains in sleep mode to save the energy. Every sensor integrated with small 8 bit microcontroller or 64 bit microprocessor. They have limited data storage capability; typically the size of RAM is of few kilobytes. When WSNs node put open in front of the world, it is very much difficult for the WSNs node to cop up with multiple events and user at a time with its bounded resources.

2.6 Security

WSNs node is not fundamentally secure [12]. They are deployed in the event prone area: either into the event or near to the event. It uses wireless channel for data transmission. Any malicious adversary can wield the node as per their malevolence intensity. Here we talked about the particular region of the WSNs but when we talked about the integration of the WSNs with the IoT, we open the access of the node to the world. IoT is very much vulnerable for the external attack [13–15]. Integration implies that now the WSNs node is also suffers from the same vulnerability as shown in **Figure 9**. The attacker would able to threaten the WSNs from anywhere in the world. Any malware from the internet can create an adverse effect on the functionality of the WSNs.

- Malicious Node Attack: In this type of attack, an attacker can create a malicious node among two nodes or more than two nodes as shown in **Figure 10**. Node A is sending some data to node B via node C. An Adversary first inserts the replica of node C into the network. This malicious node will alter the communication path between a sender and a receiver. Now the malicious node C can access all the data and can modify it for its malicious intense. The attacker can use multiple malicious nodes for this attack [16].

- Sink Hole Attack: In a sink hole attack, an attacker first compromise one node in the sensor network and through that it propagate fake information about the routing information. By sending the fake routing information it attracts traffic from the network. Once it has access the data it can alter it or can drop some data. Moreover, it also increases the energy consumption in network

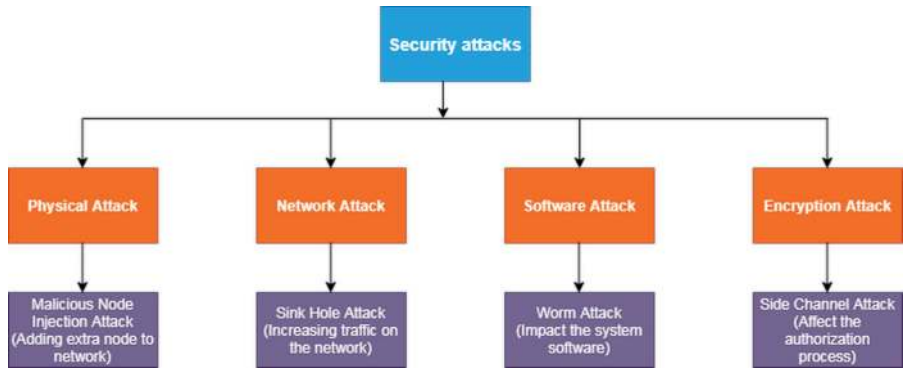

Figure 9.
Security attack on WSNs.

by unnecessary communication. That is indeed a critical situation for energy scary network like WSNs (**Figure 11**).

- Warm Attack: In a warm attack, an adversary can degrade the system operation by corrupting the system software. It is implied by the malicious code in the node. Once the node becomes the victim of a warm attack it can be denying its service to the neighbor, modifying the information, or may get access to important information. Warm is capable to reproduce itself.

- Side Channel Attack: This kind of attack wreck the encryption mechanism and get the private key. The attacker breaches the side channel information. Side channel information contains timing information, power consumption or electromagnetic leaks. Catch attack, timing attack, power monitoring attack, acoustic crypto analysis are some of the example of side channel attack.

One solution to that is WSNs must be protected by the powerful gateway. This solution is not feasible in the current infrastructure as it comes with scarce resources in the WSNs [17–20]. It is sheer essential to provide fundamental security measures to the sensor node while connecting to the internet [21]. We can use encryption techniques like symmetric key encryption model or public key encryption model for the communication. To implement the encryption model, it requires a secure key infrastructure that can provide a secure key for communication. It seems fascinating but it is a strenuous task to implement the encryption model in WSNs which comes with a large number of nodes. Moreover, it adds extra overhead to the communication which is an undesirable condition, especially with scarce

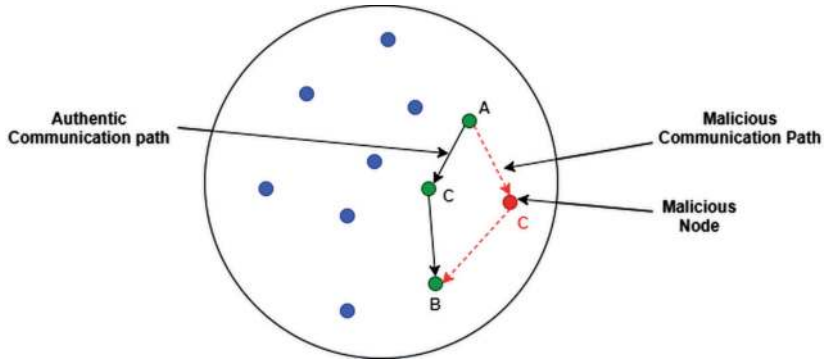

Figure 10.
Malicious node injection.

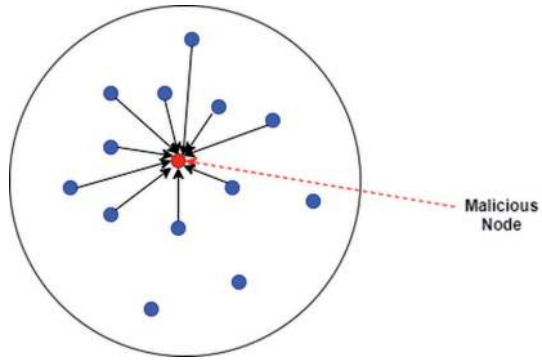

Figure 11.
Sink hole attack.

resources. It is also required deliberate dealing with the switching of sensor node between sleep mode and active mode [22].

When a sensor node connects with any internet host (human or machine) the first task is to provide authentication to the user. Internet user must need to prove his identity that he/she is the right person who collects the data whereas node must need to assure that it offers it services to the right client. There are certain scenarios where the level of authorization varies with the user, i.e. a public space like a library where any user can access the data on the other side, in a private organization or in a defense organization only a limited person can access the data [23].

Another important aspect is to keep a record of communication to enhance security. The internet is full of the heterogeneous user. When we integrate WSNs with the internet, we are opening the doors of WSNs to heterogeneous users. They can access data as well as modifying the data. The internet has an abundant amount of resources. They can store the communication detail in a large server, but on the other side sensor node comes with limited resources. It is very much difficult for the sensor node to keep track of all the communication. Consequently, it is mandatory to find a mechanism to store that data either at the node or in a special server [5, 24].

3. Conclusion

Integration of IoT and WSNs enables the broad opportunity in almost every aspect of the life. The integration seems fascination at first look but it comes with unseen challenges. In WSNs, sensor node is equipped with very low resources in terms of hardware as well as software. Operating system of the sensor node has very low processing capacity and its operation is quite different from the internet node. Hardware of sensor node is designed in such way that it consumes less energy and comes in to active mode as and when any event happens. On the other hand IoT has no limitation either in processing capability or hardware compatibility. In the integration, the layered function of WSNs and IoT has to be tailored for the interoperability. Moreover, WSNs node needs to be updated to deal with the security attacks from the internet. Overall for the faithful integration WSNs has to upgrades it capacity and IoT needs to tailor its layered operation so that it can be compatible with WSNs.

Author details

Brijesh Kundaliya
C S Patel Institute of Technology, CHARUSAT University, Changa, India

*Address all correspondence to: kundaliyabrijesh@yahoo.com

References

[1] Kundaliya, B.L. and Hadia, S.K., 2020. Routing Algorithms for Wireless Sensor Networks: Analysed and Compared. Wireless Personal Communications, *110*(1), pp. 85-107.

[2] CV Networking. Cisco Global Cloud Index: forecast and methodology, 2016-2021 White Paper. San Jose, CA, USA: Cisco Public; 2018

[3] Sharma, R., Prakash, S. and Roy, P., 2020, February. Methodology, Applications, and Challenges of WSN-IoT. In *2020 International Conference on Electrical and Electronics Engineering (ICE3)* (pp. 502-507). IEEE.

[4] Roman, R. and Lopez, J., 2009. Integrating wireless sensor networks and the internet: a security analysis. Internet Research, *19*(2), p. 246.

[5] Christin, D., Reinhardt, A., Mogre, P.S. and Steinmetz, R., 2009. Wireless sensor networks and the internet of things: selected challenges. Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose sensornetze, pp. 31-34.

[6] Haque, M., Asikuzzaman, M., Khan, I.U., Ra, I.H., Hossain, M. and Shah, S.B.H., 2020. Comparative study of IoT-based topology maintenance protocol in a wireless sensor network for structural health monitoring. Remote Sensing, *12*(15), p. 2358.

[7] Shahraki, A. Taherkordi, A. Haugen, Ø. And Eliassen, F.,2020 "A Survey and Future Directions on Clustering: From WSNs to IoT and Modern Networking Paradigms," in *IEEE Transactions on Network and Service Management*, doi: 10.1109/TNSM.2020.3035315.

[8] Ever, E., 2019. Performability analysis methods for clustered WSNs as enabling technology for IoT. In *Performability in Internet of Things* (pp. 1-19). Springer, Cham.

[9] Lohan, V. and Singh, R.P., 2017, October. Research challenges for Internet of Things: A review. In *2017 International conference on computing and communication technologies for smart nation (IC3TSN)* (pp. 109-117). IEEE.

[10] Luckenbach, T., Gober, P., Arbanowski, S., Kotsopoulos, A. and Kim, K., 2005, June. TinyREST-a protocol for integrating sensor networks into the internet. In *Proc. of REALWSN* (pp. 101-105).

[11] Kundaliya, B. and Hadia, S.K., 2020. M-RPSS: A modified RPSS for path scheduling of mobile sink in wireless sensor network. International Journal of Communication Systems, *33*(7), p.e4335.

[12] Karabiyik, U. and Akkaya, K., 2019. Digital forensics for IoT and WSNs. In *Mission-Oriented Sensor Networks and Systems: Art and Science* (pp. 171-207). Springer, Cham.

[13] Rani, S., Maheswar, R., Kanagachidambaresan, G.R. and Jayarajan, P., 2020. *Integration of WSN and IoT for Smart Cities*. Springer International Publishing.

[14] Butun, I., Österberg, P. and Song, H., 2019. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, *22*(1), pp.616-644.

[15] Sobin, C.C., 2020. A Survey on Architecture, Protocols and Challenges in IoT. *Wireless Personal Communications*, pp.1-47.

[16] Deogirikar, J. and Vidhate, A., 2017, February. Security attacks in IoT: A survey. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) (pp. 32-37). IEEE.

[17] Walters, J.P., Liang, Z., Shi, W. and Chaudhary, V., 2007. Wireless sensor network security: A survey. Security in distributed, grid, mobile, and pervasive computing, *1*(367), p.6.

[18] Dierks, T. and Rescorla, E., 2008. RFC 5246-the transport layer security (TLS) protocol version 1.2. *The Internet Engineering Task Force (IETF)*.

[19] Eronen, P. and Tschofenig, H., 2005. RFC4279: Pre-shared key ciphersuites for transport layer security (TLS). *Internet Engineering Task Force*.

[20] Park, J., Gofman, M., Wu, F. and Choi, Y.H., 2016. Challenges of wireless sensor networks for Internet of thing applications.

[21] Pundir, S., Wazid, M., Singh, D.P., Das, A.K., Rodrigues, J.J. and Park, Y., 2019. Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. IEEE Access, *8*, pp.3343-3363.

[22] Viswanathan, A., Shibu, N.S., Rao, S.N. and Ramesh, M.V., 2017, December. Security Challenges in the Integration of IoT with WSN for Smart Grid Applications. In *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1-4). IEEE.

[23] Matharu, G.S., Upadhyay, P. and Chaudhary, L., 2014, December. The internet of things: Challenges & security issues. In *2014 International Conference on Emerging Technologies (ICET)* (pp. 54-59). IEEE.

[24] Shafique, K., Khawaja, B.A., Sabir, F., Qazi, S. and Mustaqim, M., 2020. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. IEEE Access, 8, pp.23022-23040.