RESEARCH REVIEW JOURNALS
Volume-04
Issue-01
January -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Advance and Efficient Techniques for Wireless Sensor Networks Security

[1]Sushila Rani & [2]Dr Mukesh Kumar

[1,2]*The technological Institute of Textile & Sciences, Maharshi Dayanand University (India)*

ARTICLE DETAILS

Article History
Published Online: 10 January 2019

Keywords
WSN, PACKET, NODE, ERROR RATE, IDS, IP

ABSTRACT

Wireless Sensor Networks [1] is wireless state network that have free tools using the sensors to verify the corporal and the ecological terms. Such systems are integrating the opening which also gives wireless level attachment rear to the wired level world and circulated knots. This research paper has introduced the wireless sensor network with Protocol Layer Stack. Several researches focusing on Wireless Sensor Network Challenges along with its Possibilities have been discussed in this paper. Research has proposed advance and efficient techniques in order to make comparative analysis of error rates at the time of transfer data and time taken to transfer packet in case of traditional and proposed work.

1. Introduction

Wireless Sensor Networks [1] are considered as the wireless state network which consists of mainly the isolated free tools using the sensors to verify the corporal and the ecological terms. WSN system integrates the opening which also gives wireless level attachment rear to the wired level world and circulated knots.

The most challenging objective in Wireless Sensor Networks [2] is generating minimum costing as well as small sensor nodes. The Wireless [3] Sensor Network converses with Local Region Network or Wide Region Network by a gateway in many applications.

Architecture of sensor node in WSNs

In architecture of sensor node [4] Wireless sensor node is finished up of the 4 simple components and the first one is sensing component, second one is processing component, third is transceiver component and the fourth is power component. There could be the request dependent supplementary parts such as the location ruling scheme and a power generator.

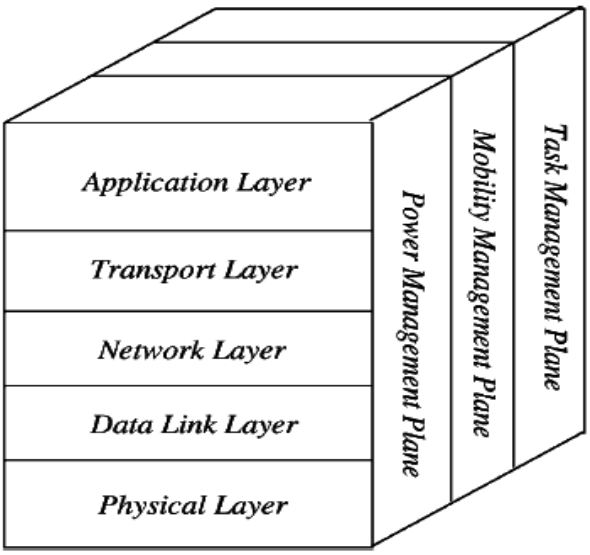

Fig 1 Protocol Layer Stack of WSNs [5]

Followed by the Open Source Interconnection (OSI) Reference model, comes the most common architecture for sensor networks. We need five layers in a sensor network basically which include the application layer, the transport layer, the network layer, the data link layer and the physical layer as shown in figure1.

Sensing Components: - Sensing components are typically composed of two sub-units: sensor[6] and A-D Converters. Sensor is that the tool which is in use for translating physical movement to the electrical signs.

Processing Component: - Processing component primarily offers cleverness to sensor node. Processing Component is consisting of micro-processors that are responsible to manage sensors. It is also performing communication protocols [7] implementation and the signal dispensation process on stored sensor based data.

Transceiver Component: Radio is allowing wireless communication with the nearest nodes in the outer world. This comprises a radio with small range that is generally having one channel at small rate of data and functions at the bands with no license of 870 mega hertz, approximately 910 mega hertz or near about 2.4 GHz.

Backup Battery: The battery is supplying the energy to sensor node completely. This is also playing a very important function during shaping of the sensor node forever. Addition of the power strained from a backup battery must be cautiously observed.

2. Literature Review

This chapter includes literature survey, to get basic information and find scope of investigation, to develop Wireless Sensor Network for optimization of its different parameters such as lifetime of network, delivery ratio of packets, loss ratio of packets and along the length delay.

The author Amit Rathee et. al. (2016) describes Wireless Sensor Network Challenges along with its Possibilities [1].

This paper is much helpful for a newbie in the area of WSN. Also, this paper puts advance WSN area fully but a bit more complete explanation could be there for each protocol precisely in upcoming days.

The author Priyanka Rawat et. al. (2014) describes about the latest advancements and possible synergy in WSNs.

WSN has materialized as one of the main capable technologies for the future [2]. This has become possible by the advancement in the technology and accessibility of very small, low-cost and quick sensors resulting in the cost efficient and easily deployable networks.

The author Phuntsog Toldan et. al. (2013) proposed Design Issues and a variety of Routing Protocols for WSN [3].

In case of MSN, node gathers information by turning from one position to another position. Thus localization is required. MSN are further power effective, enhances targeting and offers higher information loyalty than the Static Sensor Network.

The author Sanjeev Kumar Gupta et. al. (2014) discussed Overview of Wireless Sensor Network [5].

The paper provides the past of WSNs. In starting an architectural overview of a SN, protocol stack, networking standards, performance modeling of the WSN through the radio power model is described.

The author Divya Sharma et. al. (2013) presented a review on Network Topologies in WSNs.

Research work explains the topology of network. Sensing nodes have constrained power source energy, so consumption of the energy is necessary issue.

The author Vineet Bansal et. al. (2012) described latest bandwidth proficient and network dependent on Demand Routing Protocol which is used for MANETs.

Precisely, lack of a central approval service in an open and disseminated interaction situation is a big question to be answered. In MANETs, any of the nodes may negotiate routing procedure functionality and for this the route detection procedure is disrupted.

The author Sang Jin Lee et. al. (2008) described about determining technique for Dynamic Filtering in case of Wireless Sensor Networks that uses Fuzzy Logic.

This paper represented a fuzzy based entrance that would be required to determine the methods for dynamic en-route method for filtering artificial data injection in wireless sensor networks.

The author Jamal N. Al-Karaki et. al. (2009) put forward Data Aggregation and Routing in case of Wireless Sensor Networks.

In this Survey focus is on routing protocols which may vary according to application and network architecture. In this research a survey of state of art routing technique in case of Wireless Sensor Networks has been presented.

The author Aamir Shaikh et. al. (2012) discussed on Wireless Sensor Network Technology Research.

A System consisting of management system database as well as ZigBee network, has several essential benefits which include cost effectiveness, less consumption of power, small rate of data transmission etc.

The author Edwin Prem Kumar Gilbert et. al. (2012) described Research Issues in Wireless Sensor Network Applications.

This paper reflects the introduction of different research problems in WSN applications. Also, summary of wide spectrum of requests of WSN has been represented in the paper. The applications of WSNs in the regions of intelligent parking, biomedical, armed, industrial and healthcare application has been briefed.

The author Lucas Leão et. al. (2014) explained the term FLBRA: Fuzzy Logic Based Routing Algorithm for Indoor WSNs.

Considering situation of the building administration systems with the WSN observing environmental facial manifestation, this following paper represents a scheme of FLBRA to decide value of every link and recognition of finest ways for packet forwarding.

The author Zainab H. Fakhri et. al. (2014) describes about the Performance Analysis of Dynamic Wireless Sensor Networks by the method of Linguistic Fuzzy.

In this paper a comparison between Linguistic Fuzzy Trust Model and Bioinspired Trust and Reputation Model for Wireless Sensor Networks is attained in the requisites of precision and average trail length.

The author Madhumita Panda (2014) discussed on Security in Wireless Sensor Networks by means of Cryptographic Techniques.

Two different schemes ECC and RSA have been contrasted in this paper and it is concluded that ECC is beneficial as judged against RSA. This is due to the very less memory being used, very small CPU utilization and smaller key size as equated to RSA.

The author Nibedita Priyadarshini (2015) presented a method for Improving Life of WSN by means of Energy Harvesting Clustering.

Authors proposed power harvesting leach model enhances the lifespan of the network that appears to be away from the level which all accepted.

The author R. Rathna et. al. (2015) proposed centralised in the opponent to the dispersed medium access control arrangement for the environmental examining sensors [18].

Both the centralised and distributed MAC arrangement protocols have their own benefits and drawbacks.

3. Tools & Technology

In case of Intrusion detection there are several problems with existing system. Usually data is transferred from one IP to

another IP using most commonly used protocol such as FTP, TELNET, and HTTP.

Here we have used our own protocol to send the data as we have used port no above 1024, here we have not used reserved port number for data transmission.

Second thing is that the probability of success of attack increases when data is large in size and sent as it is. So we have reduced the size of packets by exchanging contents of data file with some short words during send and original words are restored at receiving end.

If huge Number of packets sent on common route then it becomes difficult to save data from intrusion detection attack.

Third option is to reduce the number of packets in queue so that during routing it becomes easy to secure the packets from intrusion detection.

Use of User datagram protocol makes the transmission un reliable because there is no confirmation in this case so we have use TCP based data transmission protocol in our research.

Client Server Model

It is possible for two network applications to begin simultaneously, but it is impractical to require it. Therefore, it makes sense to design communicating network applications to perform complementary network operations in sequence, rather than simultaneously. The server executes first and waits to receive; the client executes second and sends the first network packet to the server.

Overview Of IP4 Addresses:

IP4 addresses are 32 bits long. They are expressed commonly in what is known as dotted decimal notation. Every of the four bytes which makes up the thirty three address are expressed as an integer value and separated by a dot. For example, 138.23.44.2 is an example of an IP4 address in dotted decimal notation.

Port

Sockets are UNIQUELY identified by Internet address, end-to-end protocol, and port number. In our labs we will basically be working with TCP sockets [11]. Ports are software objects to multiplex data between different applications. When a host receives a packet [7], it travels up the protocol stack and finally reaches the application layer. To which application should the packet be delivered? Well part of the packet contains a value holding a port number [9], and it is this number which determines to which application the packet should be delivered. So when a for many common services, standard port numbers are defined.

Packet [3] consists of port number & IP address where data is to be delivered within data.

Port number1 to 1023 are reserved for existing services but 1024 to 65535 are available for our programs.

Tools in intrusion detection

An intrusion detection product available today addresses a range of organizational security goals [2].This section discusses about security tools.

SNORT

Snort is lightweight & open source software. Snort uses a flexible rule-based language to describe traffic [6].From an IP address; it records packet in human readable form._Through protocol analysis, content searching.

OSSEC (open source security) is free open source software. It would run on major operating system & uses a Client/Server based architecture. OSSEC has ability to send OS logs to server for analysis & storage. It is used in powerful log analysis engine, ISPs, universities & data centres. Authentication logs, firewalls are monitored & analyzed by HIDS.

FRAGROUTE

It is termed as fragmenting router. Here, from attacker to fragrouter IP packet is sent and they are then fragmented & transformed to party.

Honeyd is a tool that creates virtual hosts on network [6]. The services are used by host Honeyd allows a single host to request multiple addresses on a LAN for networks simulation. It is possible to knock virtual machines or to trace route them [6]. Any type of service on virtual machine can be simulated according to a simple configuration file [6].

KISMET

It is a guideline for WIDS (Wireless intrusion detection system. WIDS compromises within packet payload & happenings of WIDS. It would find burglar access point.

4. Proposed Work

The purpose of proposed is to boost data transmission speed over network without introducing any new hardware. To do this we have to understand reasons of delay in data transmission. Proposed work is focusing on following objectives:

1. Establishment of Network Environment to test flow of packets
2. Development of packet sender & receiver module.
3. Simulation using GNS3 and node creation.
4. Development of Intrusion detection System
5. Testing transmission delay in packet transmission due to security for IDS
6. Testing processing delay during packet transmission
7. Testing queuing delay of network packets
8. Testing propagation delay at time of data transmission

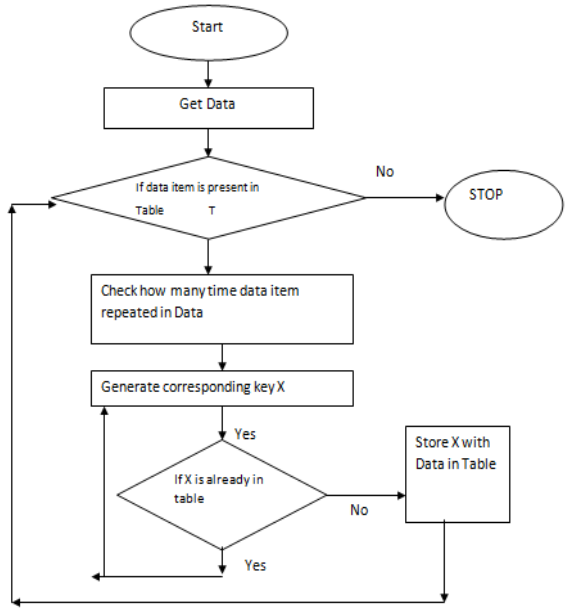

Fig 2 Packet Size Reduction Logic

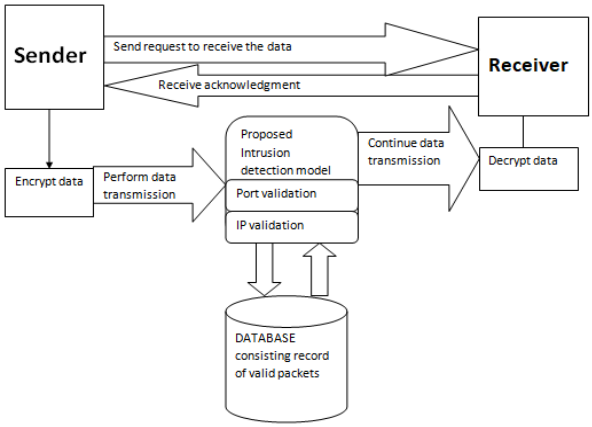

Fig 3 Proposed Intrusion Detection Model

5. Result Analysis

Comparative analysis of time taken to transfer packet

The fig 4 represents the time taken during transmission of data with respect to number of packets. Here in following simulation comparative analysis between existing and proposed work has been represented. Following simulation represent that time taken are less in case of proposed work.

Result of output

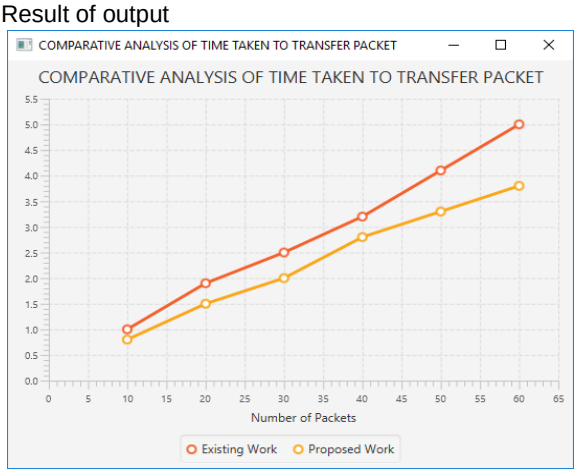

Fig 4 Comparative analysis of time taken to transfer packet

In fig 4 the Time taken during transfer of the number of packet has been considered. The x axis of graph is representing the number of packets. On other hand the y axis is representing the time taken during data transfer in case of traditional and proposed work. Here we have two cases

Case 1: Time taken in case of tradition work: In this work the time taken during transfer packet when tradition techniques have been used is considered.

Case 2: Time taken in case of Proposed work: In this work the Time taken during transfer packet during data transmission in proposed techniques have been considered. Here data has been transferred with less time as compare to traditional technique.

Comparative analysis of error rates at the time of transfer data

The fig 5 represents the error rate during transmission of data with respect to number of packets. Here in following simulation comparative analysis between existing and proposed work has been represented. Following simulation represent that errors are less in case of proposed work.

Result of Analysis

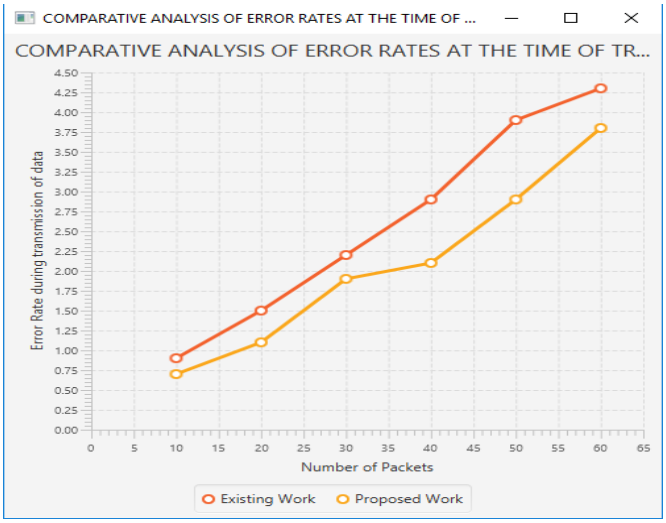

Fig 5 Comparative analysis of error rates at the time of transfer data

In fig 5 the error rates during transfer of the number of packet have been considered. The x axis of graph is representing the number of packets. On other hand the y axis is representing the error rate during data transfer in case of traditional and proposed work. Here we have two cases:

Case 1: Error rate in case of tradition work: In this work the error rate during transfer packet when tradition techniques have been used is considered.

Case 2: Error rate in case of Proposed work: In this work the error rate during transfer packet during data transmission in proposed techniques have been considered. Here data has been transferred with less error rate as compare to traditional technique

Comparative analysis of packet size

The fig 6 represents the packet size during transmission of data with respect to number of packets. Here in following simulation comparative analysis between existing and proposed work has been represented. Following simulation represents that the packet size is less in case of proposed work.

Result

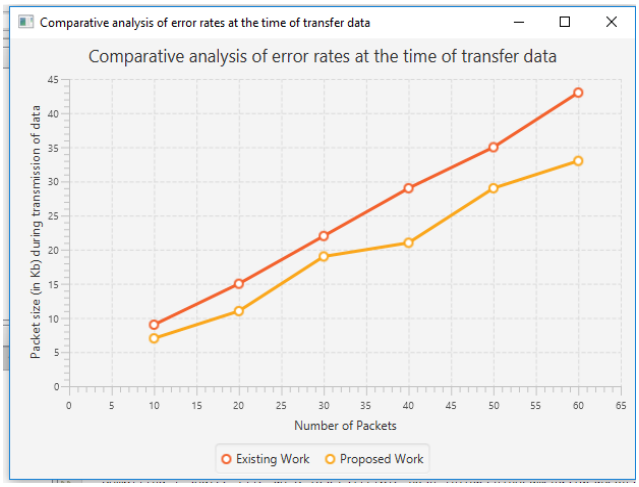

Fig 6 Comparative analysis of packet size

In fig 6 the packet size during transfer of the number of packet has been considered. The x axis of graph is representing the number of packets. On other hand the y axis is representing the packet size during data transfer in case of traditional and proposed work. Here we have two cases

Case 1: Packet size in case of tradition work: In this work the packet size during transfer packet when tradition techniques have been used is considered.

Case 2: Packet size in case of Proposed work: In this work the packet size during transfer packet during data transmission in proposed techniques have been considered. Here data has been transferred with less packet size as compare to traditional technique.

Comparative analysis of transmission time in case of secure and unsecure traditional and proposed work

The fig 7 represents the transmission time of data with respect to number of packets in case of secure an unsecure proposed work as well as tradition work. Here in following simulation comparative analysis between existing and proposed work has been represented.

Following simulation represents that the transmission time is less in case of proposed work.

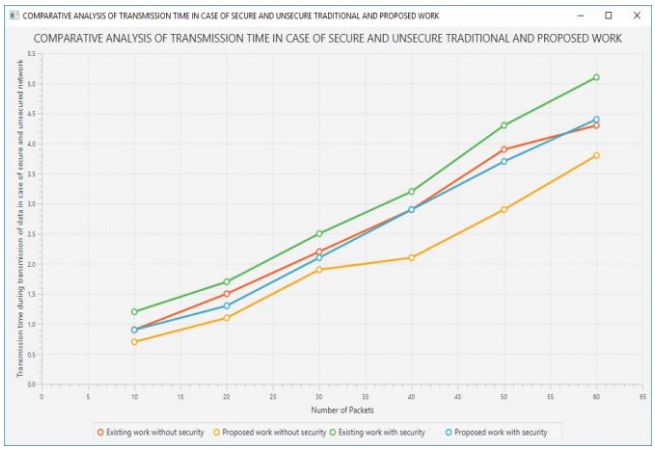

Fig 7 Comparative analysis of transmission time in case of secure and unsecured traditional and proposed work

In fig 7 the transmission time taken to transfer the number of packet has been considered. The x axis of graph is representing the number of packets. On other hand the y axis is representing the time taken to transfer data in case of secured and unsecured traditional and proposed work. Here we have four cases

Case 1: Unsecure tradition work: In this work the time taken to transfer packet when there is no security mechanism during data transmission in tradition techniques.

Case 2: Unsecure Proposed work: In this work the time taken to transfer packet when there is no security mechanism during data transmission in proposed techniques. Here data has been transferred faster as compare to traditional unsecure transmission technique.

Case 3: Secure tradition work: In this work the time taken to transfer packet when there is security mechanism integrated to it during data transmission in tradition techniques. It is taking more time.

Case 4: Secure Proposed work: In this work the time taken to transfer packet when there is security mechanism during data transmission in proposed techniques. Here data has been transferred faster as compare to traditional secure transmission technique.

6. Conclusion

Identifying trusted data sources & marking data coming from these sources as trusted, Using dynamic tainting to track trusted data at runtime, & Allowing only trusted data to form semantically relevant parts of queries such as SQL keywords & operators. Unlike previous approaches based on dynamic tainting, our technique is based on positive tainting, which explicitly identifies trusted (rather than untrussed) data in a program. This way, we eliminate problem of false negatives that might result from incomplete identification of all untrussed data sources. False positives, although possible in some cases, could typically be easily eliminated during testing. Our approach also provides practical advantages over many existing techniques whose application requires customized & complex runtime environments: It is defined at application

level, requires no modification of runtime system, & imposes a low execution overhead.

We are focusing on following objectives. So there had been need to focus on Establishment of Network Environment to test flow of packets & also need of Development of packet sender & receiver module. We had studied of existing Testing transmission delay in packet transmission & Testing processing delay during packet transmission. We also make study of testing queuing delay of network packets.

7. Future Scope

The presented work is about to improve the routing in MANET by using the concept of IDS mechanism which can provide security as required and also increase the overall life time of the network by diminishing the power consumption by the node is required. For optimum the local node we divide the network in smaller zones and identify the virtual coordinator over the zone. This coordinator will contain the communication statistics of zone nodes. As the routing will be performed, the effective hop selection will be done by the virtual coordinator.

References

1. Rathee, A., Singh, R., & Nandini, A. (2016). Wireless Sensor Network-Challenges and Possibilities. International Journal of Computer Applications, 140(2).
2. Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. The Journal of supercomputing, 68(1), 1-48.
3. Toldan, P., & Kumar, A. A. (2013). Design Issues and Various Routing Protocols for Wireless Sensor Networks (WSNs). In Proceedings of National Conference on New Horizons in IT-NCNHIT (p. 65).
4. Sharma, S., & Mittal, D. P. (2013). Wireless Sensor Networks: Architecture, Protocols. International journal of advanced research in computer science and software engineering, 3(2).
5. Alkhatib, A. A. A., & Baicher, G. S. (2012). Wireless sensor network architecture. In 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012).
6. Gharajeh, M. S., & Khanmohammadi, S. (2016). DFRTP: Dynamic 3D Fuzzy Routing Based on Traffic Probability in Wireless Sensor Networks. IET Wireless Sensor Systems, 6(6), 211-219.
7. Gupta, S., K., & Sinha, P. (2014). Overview of Wireless Sensor Network: A Survey. International Journal of Advanced Research in Computer and Communication Engineering, 3(1), 5201-5207.
8. Tiwari, P., Saxena, V. P., Mishra, R. G., & Bhavsar, D. (2015). A survey of localization methods and techniques in wireless sensor networks. HCTL Open International Journal of Technology Innovations and Research (IJTIR), 14, 2321-1814.
9. Zhao, F., & Guibas, L. J. (2004). Wireless sensor networks: an information processing approach. Morgan Kaufmann.
10. Kumar, J., & Sangwan, S. (2014). State of Art Techniques for Wireless Sensor Network Lifetime Maximization. International Journal of Enhanced Research in Science Technology & Engineering, 3(5), 275-279.
11. Othman, M. F., & Shazali, K. (2012). Wireless sensor network applications: A study in environment monitoring system. Procedia Engineering, 41, 1204-1210.
12. Kumar, D. M. (2012). Healthcare Monitoring System Using Wireless Sensor Network. International Journal of Advanced Networking and Applications, 4(1), 1497.
13. Rani, A., & Bindal, A. (2017). Review of Energy Saving Protocols in WSNs. International Journal of Advanced Research in Computer Science, 8(3), 991-995.
14. Dharmateja, M., & Vaishnavi, K. Energy Optimization In Wireless Sensor Networks Using Leach Protocol. International Journal of Wireless Communication and Simulation, 8(1), 21-30.
15. https://www.amrita.edu/center/awna/research/energy-optimization issues
16. Kaur, A., & Kaur, K. (2015). A Review of Different Energy Efficiency Techniques in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Software Engineering, 5(6), 283-288.
17. Verma, N., & Sangwan, S. (2016). Secure and Energy Efficient Routing in Wireless Sensor Networks: A Review. International Journal of Computer Science & Engineering Technology (IJCSET), 7(2), 33-37.
18. Rathna, R., Dhanalakshmi, R., & Sasipraba, T. (2015). Centralised against distributed medium access control scheduling for environmental monitoring sensors. IET Wireless Sensor Systems, 5(6), 271-276.
19. P., & Sangwan, S. (2014). Secure Hierarchical Data Aggregation in Wireless Sensor Networks – General framework. International Journal of Engineering Research & Technology, 3(6), 1015-1019.
20. Dureja, R., & Malik, M. (2015). Routing in Wireless Sensor Networks: A Review. International Journal of Emerging Research in Management & Technology, 4(10), 124-129.

