ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
https://zenodo.org/records/15835465
Vol 14, Issue 3, 2020

A SURVEY OF WIRELESS SENSOR NETWORK SECURITY

[1]Chikati Aravind Kumar, [2]Dr.Sandeep Chahal

Research Scholar, aravind.chikati@gmail.com, Department of Computer Science and Engineering, NIILM UNIVERSITY, Kaithal, Haryana, India.

[2]Associate Professor, Computer Science and Engineering, NIILM UNIVERSITY

Abstract

The main purpose of the study is to review the evolution of wireless sensor network security and routing techniques. Recent years have seen tremendous growth in Wireless Sensor Networks (WSNs). As WSN's become more and more crucial to everyday life, their security and trust become a primary concern. However because of the nature of WSNs, security design can be challenging. Trust-aware routing protocols play a vital role in security of Wireless Sensor Networks (WSNs). The review study provides an overview of Wireless Sensor Network (WSN) and discusses security issues and the routing techniques for high quality of service and efficient performance in a WSN. In order to identify gaps and propose research directions in WSN security and routing techniques, the study surveys the existing body of literature in this area. The main focus is on trust concepts and trust based approaches for wireless sensor networks. The study also highlights the difference between trust and security in the context of WSNs. The trust and security are interchangeable with each other when we elaborate a secure system and not same. Various surveys conducted about trust and reputation systems in ad hoc and sensor networks are studied and compared. Finally we summarize the different trust aware routing schemes.

Keywords: Attacks, blackhole, protocols, security, trust, WSN

I. INTRODUCTION

Technological advancements in wireless communication technologies have led to the development of inexpensive sensor nodes. The availability of these nodes has made Wireless Sensor Networks (WSN) one of the most promising technologies of the past decade. A wireless sensor network is formed by a large number of distributed sensor nodes in a particular

environment for sensing and monitoring. In most cases, these tiny sensors nodes are equipped with an antenna, radio transceiver, a processor, memory and a battery. The function of these independent nodes is monitoring, sensing and collecting data within a specific area and sending this information back to base station for analyzing. The base station acts as a gateway for connecting with end user points. Wireless communication is used to transmit data between sensor nodes and base station using a set of predefined rules called routing protocols (Abd-El-Barr et al., 2005). Due to nature of Wireless Sensor Networks, routing in a sensor network is very challenging because of many features that distinguish sensor networks from other wireless networks (Perrig et al., 2004; Akkaya and Younis, 2005; Nivetha and Venkatalakshmi, 2012). As compared to wired networks, harsh deployment environment of sensor networks makes them vulnerable to physical and logical security attacks. Various types of routing protocols have been proposed for WSNs however none of them completely secure the sensor nodes (Boukerche et al., 2011). A WSN is characterized by its broadcast nature, frequently changing topology, unsupervised manner of operation and transmission medium. These factors make the design of routing protocols very challenging. In presence of these factors routes are easily discontinued. Additionally links between nodes may have limited bandwidth, limited energy and stringent resources (Kohno et al., 2012). The secure routing protocols should be lightweight and minimize energy consumption and complexity. One of the main concerns in WSN applications is to design a secure routing protocol that is able to operate in a harsh and unattended environment. Security is one of the most important and useful metric for routing protocols (Nikjoo et al., 2007). A secure routing protocol ensures connectivity in the presence of node failure and security attacks. In this study, we present the evaluation of some popular and well-known wireless senor network routing protocols with their security techniques and study their limitations and strengths in detail.

II. MATERIALS AND METHODS

Model of wireless sensor network: The wireless sensor network consists of many nodes and every node independently senses and computes in the network. The nodes in network communicate and forward the sense data to a central processing unit. A commonly used sensor node is the Mica2 Mote developed by Crossbow technology. The wireless sensors are deployed densely and with limited resources in a network. The topology of a network is changing constantly and uses broadcast communication medium. The sensors are not based on global

identification tags (Sharma et al., 2009). The main components of network are sensor field, sensor node, sink node and task manager. The sensor field is an area where all nodes are placed for sensing the information such as ground or a battle field. The sensor nodes are the major components and collect and forward information to other nodes. The sink nodes are called aggregation point because they have a specific task of processing, receiving and storing the data from other nodes. A sink node overcomes the energy requirement and manages the messages. In last task, manager or base station is a centralized part of network for controlling the communication. The base station is usually in the form of a laptop or computer with high processing and storage capabilities. The data is streamed via internet, wireless channels and satellite. Various sensor nodes are deployed in a field to create a wireless multi-hop network. Sensor nodes use wireless communication media such as infrared, radio, optical media or Bluetooth for their communications. Figure 1 shows the components of a sensor network.

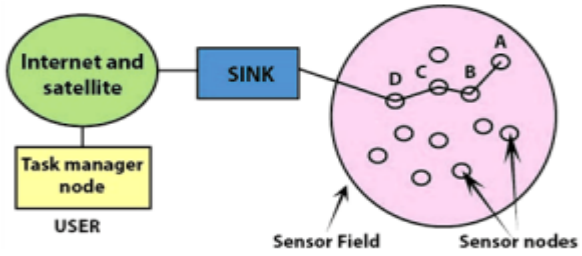

Fig. 1: Wireless sensor network components (Kaplantzis *et al.*, 2006)

Operating systems and applications: An operating system runs reliable application software and provides compatible hardware resources. The wireless sensor network operating systems are typically less complex compare with others OS because the sensor are used for special purpose and the sensor hardware has limited capabilities. The tiny OS was the first operating system specifically designed for WSN. Now a day's many OS are working in WSN nodes such as SOS (SOS embedded Operating System), LiteOS. The applications of sensor networks are valuable and practical in military as well as civilian environments. In Military, the applications can be used for battlefield monitoring, equipment and ammunition, battle damage assessment,

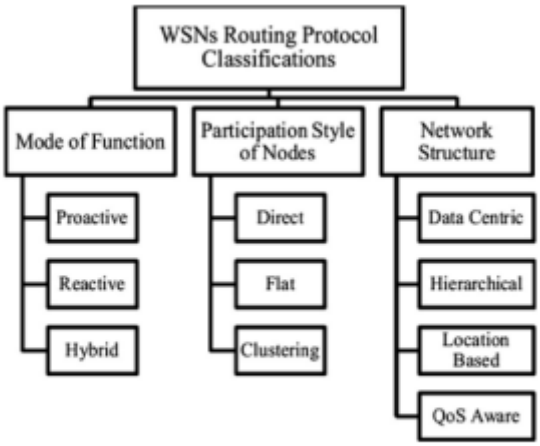

Fig. 2: WSN routing protocol classifications

targeting and reconnaissance applications monitoring. In other fields, they can be used for environmental monitoring purposes and in health applications, building automated, smart environments, such as bridges, robot control and guidance in automatic manufacturing environments, factory process control and automation, vehicle tracking and detection, monitoring disaster areas, increasing the effectiveness of agricultural processes and water management (Akyildiz et al., 2020; Buttyan and Hubaux, 2020).

Routing in wireless sensor network: This section elaborates various WSN routing protocols. Routing is a method to send the data over a network between two nodes and routing protocols are used for performing the routing. The protocols select the most efficient path for the data to reach the target node. The network layer is responsible to implement the routing of the incoming data. Most of the source nodes cannot reach to destination due to their transmission range and in this situation; the intermediate sensor nodes forward the packets. As noted before, a WSN has some constraints such as energy supply, bandwidth etc. In past a number of routing protocols have been designed for WSN, such as LEACH, Directed Diffusion, (Heinzelman et al., 2000; Intanagonwiwat et al., 2000), APTEEN (Manjeshwar and Agrawal, 2001), SPEED (He et al., 2003). These protocols mostly focused on energy consumption. The designs of protocols are tailored by application scenario and backbone of network. Based on previous work, this study focuses on secure routing protocols (Fig. 2).

The WSN routing protocols are classified based on mode of functions, network structure and participation styles of sensor nodes. The mode of function protocols can be proactive, reactive or

hybrid. In participation mode the protocols could be flat, direct and clustering based. In network structure mode protocols can be datacentric, location based, hierarchical or QoS (Quality of Service) based.

Mode of function based protocols: The first classification of WSN routing protocols is based on mode of function and these modes are proactive, reactive and hybrid (Niezen et al., 2007). In proactive protocols, the routing table is generated at every node and the routing information of complete network is periodically updated. Pre-provisioning is also done for all possible paths for the entire network topology. In this approach, the data traffic can be sent out to its destination immediately, without the delay imposed by route acquisition in reactive protocols. However, a certain amount of control traffic is needed to keep routing tables up to date and reliable over the entire network. This control traffic is always present, independent of data traffic on the network. In reactive routing protocols no routing table is generated and route discovery is done as required. The routes between nodes are attained on demand. The source node triggers a route discovery request through the network and waits for a response from the destination node. Sometime this process takes time and causes a delay in network and overhead control depends on the data traffic in the network. By acquiring routes on demand, a node has only a partial knowledge about the network, as routes are computed only for destinations to which data traffic has to be forwarded. This might be advantageous in terms of state, as reactive protocols do not require each node to store routes for the entire network. The combination of reactive and proactive protocols is called hybrid. The hybrid approach decreases the cost of the network. It first computes all routes and then improves routes at the time of routing.

Participation style of nodes based: The second classification is participation style of nodes and in this category, three types of routing protocols are: direct, flat and clustering present (Pal et al., 2010). The direct type is based on sending all information directly to the base station. In flat type the nodes primarily find a valid route to the base station and then forward the packets to sink node or other nodes through routing responsible for collecting and communicating the data with the sink node such as Sensor Protocols for Information via Negotiation (SPIN) (Heinzelman et al., 1999), Direct Diffusion (DD) and Rumour Routing (Intanagonwiwat et al., 2000; Braginsky and Estrin, 2020). In clustering types the area is divided into number of small clusters. In which cluster head directly communicates with base station.

Network structure based protocols: The third classification is network structure type and in this category the protocols types are: data centric, hierarchical and location-based and QoS aware based (Abd-El-Barr et al., 2005). The data centric protocols depend on the tag or naming of the desired data and are responsible for eliminating redundant transmissions. In this category, the target node sends queries requesting certain data from the nodes in the network and if data matches the query, it sends them back to the requesting node. This process is belonging falls under the query based routing approach and is also known as Directed Diffusion. The examples of query based routing protocols are Directed Diffusion (DD), COUGAR (Yao and Gehrke, 2020), Sensor Protocols for Information via Negotiation (SPIN). The hierarchical based protocols perform energy efficient routing and select higher energy nodes for processing and send the information to cluster head while low energy nodes sensing the proximity of the target (Zhan et al., 2009). These types of protocols perform energy-efficient routing in WSNs and are best for reducing the amount of overall message transmissions. The most popular routing protocols in this category are Low Energy Adaptive Clustering Hierarchy (LEACH) (Heinzelman et al., 2000), Power-Efficient Gathering in Sensor Information Systems (PEGASIS) (Lindsey and Raghavendra, 2020), Threshold-sensitive Energy Efficient sensor Network protocol (TEEN) (Manjeshwar and Agrawal, 2020), Adaptive Periodic TEEN (APTEEN) (Manjeshwar and Agrawal, 2001) and Small Minimum Energy Communication Network (MECN) (Rodoplu and Meng, 1999). The locationbased protocols require location information of sensor nodes usually accessed from GPS (Global Positioning System) signals or received radio signal strength. In this category, the routing protocols work on their location for calculating the distance to its neighbor node from the incoming signal strength. To save energy in network the nodes use active or sleep state, in active state the node is alive and in sleep state the node rests if there is no activity. In some location-based schemes in order to save energy, the nodes must change their state between active or sleep. The most popular routing protocols in this category are Geographic Adaptive Fidelity (GAF) (Xu et al., 2001) and Geographic and Energy Aware Routing (GEAR) (Yu et al., 2001). The Quality of Service (QoS), aware routing focuses on many network layer requirements such as reliability and latency. The sensor network is based on balance function and quality of network, energy efficiency and data quality. In particular, the sensor networks need some quality of service metrics such as delay, energy, bandwidth, for delivering data. The popular protocols that fit in this category are SPEED (Stateless Protocol for

Real-Time Communication in Sensor Networks) (He et al., 2003) and Sequential Assignment Routing (SAR) (Sohrabi et al., 2000) (Fig. 3)

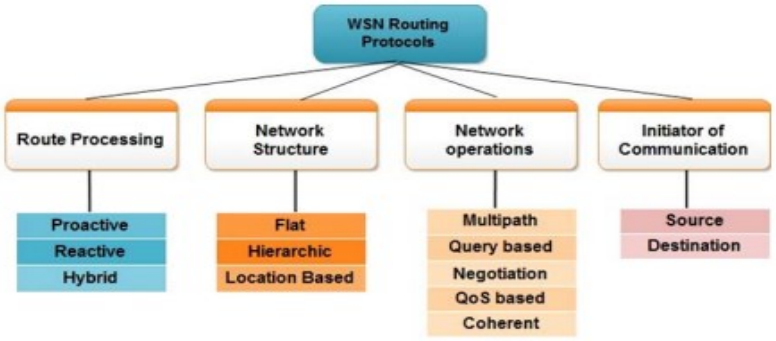

Fig. 3: Classification of WSN routing protocols

Design requirements and challenges: The existing routing protocols employ different strategies for securing routing operations in network. In WSN the nodes run routing protocols in a self-organized manner and have a dynamic topology. This section discusses the detail about design and properties which need to be satisfied to ensure security. Due to the insecure nature of sensor nodes such as ease of deployment, broadcast communication and low cast device, the security requirement is essential to protect the network from potential attackers or intruders.

Security in wireless sensor network: The advancement in wireless sensor networks has proved that they provide various advantages over traditional methods. One of the main challenges is provision of security in the network because of the possibility of the presence of one or more faulty and malicious nodes in the network (Al-Karaki and Kamal, 2004). The sensor node is at risk because of attackers that capture the node secret keys; this is referred to as insider attack (Srinivasan et al., 2009). Several security challenges have been discussed in different literature reviews such as Perrig et al. (2004), Pathan et al. (2006) and Wang et al. (2006). In security attack, an adversary node would appear to be a legitimate member of the network. When the node is captured, an adversary may sniff and inject packets with falsified data and may reprogram the sensor node and carry out system faults and bad routing by malicious nodes, which may eventually prove detrimental to the overall system. Because of these attacks, the security is a main issue, which must be addressed for a secure network. There are some external attacks in WSN that are addressed by the use of cryptographic techniques but this technique is not effective against the internal attacks by a malicious node. Nodes do not support the heavy

computations of cryptography-based protocols because the nodes are constrained by their limited resources. Efficient security protocols that are resource economical, capable to provide protection at node-level and meet the security demands of the application are required. Recently the basic ideas of trust and reputation have been applied to WSNs for monitoring changing behaviors of nodes in a network. Reputation and trust are two very useful tools that are used to facilitate decision making in diverse fields from an ancient fish market to state-of-the-art e-commerce (Srinivasan et al., 2009). Trust and security are interchangeable concepts in wireless sensor networks. Security is different from trust because security means no one is trusted and requires authentication all the time and this leads to very high overhead, while, trust means everybody is trusted somehow and does not require authentication (less overhead) (Momani, 2010). The trust and security based approaches have gained global recognition in WSNs (Khalid et al., 2013). Trust Reputation Models (TRM), deals with the problem of uncertainty in decision-making, by keeping the history of a node's previous behavior (repute). A node is trusted and will be forwarded with the packets only if the node holds a good repute; otherwise, the node will be considered untrustworthy. The same concept is applied in Trust Reputation Models (TRMs); a node will prefer to interact with a well-reputed neighboring node.

Security objectives: Security is one of the essential factors in any real time application. In data exchange phase it can greatly affect the whole network. During designing of a WSN the security attributes must be considered. The WSN has unique characteristics like wireless communication medium, resource constrained capability, dynamic topology and these characteristics open WSN for different attacks. The adversaries easily eavesdrop, inject, intercept or alter the transmitted messages. Before deploying WSN the security precautions must be taken into account. The security is important when every source node sends packets to destination nodes. WSNs are prone to different types of attacks, some important security objectives that must be considered in designing a WSN network include authentication (Sen, 2009), integrity (Burgner and Wahsheh, 2011), confidentiality, availability (Stavrou and Pitsillides, 2010) and freshness (Sen, 2009).

Security attacks in wireless sensor network: In past various type of WSN routing protocols were designed without considering security functionalities (Yahya and Ben-Othman, 2009a, b; Guo and Zhong, 2010), an adversary can set up diverse of attack on the network such as data forgery, Denial-of-service and node capture attacks (Wood and Stankovic, 2020; Perrig et al.,

2004). Moreover, the security attacks can focus on different goals of sensor network. The basic goal of attackers is to disturb and completely paralyze the routing operation. The node security is a significant need in the network and a malicious node can collapse the whole network at worst, beside the disclosure of some vital network information. The attacks can be classifies in different ways but main categories are passive and active attacks (Deng et al., 2020). In passive attacks the information is transmitted by eavesdropping without disrupting the routing protocol operations. The active attacks can be classified into internal and external types. The node misbehaves in many different ways and can become resource deficient. Therefore, we must understand the various types of node misbehaviors that WSNs may usually encounter. There are two common types of misbehaving nodes (Cho et al., 2011) selfish and malicious nodes. The selfish node does not cooperate with other nodes because of some resource constraint like low battery. A selfish node may have no intention to cause harm to the system. There is also a possibility that an adversary reprograms a captured node to act selfishly. The malicious node has an intention to cause maximum harm to the system, even at the cost of node's own resources. There are many types of node misbehaviors such as gray hole, black hole, routing loop, bad mouth, wormhole etc. In gray hole attack the malicious node choose the packet on the base of packet type. The malicious node may not forward the active data packet in network but may participate in routing by forwarding the routing packets. In black hole misbehavior the malicious node advertises wrongly that it has a shortest route to the destinations. After receiving the packet malicious node drops the packet. In routing loop misbehavior, the malicious node changes route information and causes routing loop in network. The routing loop may cause congestion and denial-of-service issues in network. Some malicious nodes may get together to spread false information about a normal node. Therefore, the trust rating of a well-reputed node may reduce. In wormhole misbehavior, some nodes make a group and redirect traffic to a slow link that may cause congestion and increased latency in the network. The malicious node delays packets randomly in network and this behavior keeps the trust rating of the node above a certain threshold. Therefore, the malicious node may not be detected easily. The packet may be injected, with wrong data, such as false source and destination identifiers. In Sybil attacks, the node masquerades its identity to appear with multiple identities to represent more than one node. Therefore, it is difficult to detect such a node acting maliciously when the node is frequently changing its identities. In transient behavior a node may alternate between the roles of being on and off to

keep the repute of the node above a certain threshold. Therefore, making it hard to detect a malicious node. In ID spoof an intruder may alternatively spoof the source ID of the routed packets, leading to the disruption of routing. In such a scenario, it would also be difficult to locate the intruder node. In node collision behavior one node plays different roles with different node groups. It can sometime misbehave with one group and behave well with another group. This creates an environment of mistrust between the two groups. The low battery problem is the most common example of resource constraint a node may experience in a WSN. A node with low battery may participate in the route discovery process. However, the node may decline participation in packet forwarding, which renders the node indistinguishable from the packet dropping malicious nodes. The Black hole attack is misbehavior of a node in network. A Black hole node claims itself as a suitable node for forwarding the packets to destination in the network, but actually causes dropping of packets in the network. A malicious node exploits the weaknesses of the route discovery packets of the on demand protocols, such as AODV, to drop all the packets in the network. Figure 4 shows the Black hole attack. During the route discovery in the process of AODV protocol the intermediate nodes are accountable to find a fresh path to the destination, sending discovery packets to the neighbor nodes. When source node sends RREQ packet and Node 3, a malicious node, sends a false response to the request packet that it has the shortest route to the destination. Therefore, node1 sends its data packets via the malicious node (node 3) to the destination (node 4) assuming it is a true path. As discussed above, a malicious node most likely drops the packets, so node 3's behavior can be regarded as a Black hole problem in WSN. Due to this misbehavior, node 3 is capable of misrouting the packets easily. This type of attack severely diminishes the packet delivery ratio.

CONCLUSION

This study is a part of an ongoing study on security and trust aware routing schemes. In this study, the various components of the research problem were reviewed. The study highlights the challenges associated with the implementation of WSN in unattended environments. It also introduces safety issues in wireless sensor networks and the need for innovative approaches, such as trust, to solve these problems. In the concept of trust, the difference between confidence and security has been discussed. Finally, a comparison of existing trust aware routing schemes is conducted and summarized.

REFERENCES

1. Ahmed, U & Hussain, FB 2011, 'Energy efficient routing protocol for zone based mobile sensor networks', proceedings of the seventh IEEE International IWCMC Conference on Wireless Communications and Mobile Computing, pp. 1081-1086

2. Ali, IA, Zurina, MH, Mohamed OZ &Ahmad, Z2017, 'A Secure Region-Based Geographic Routing Protocol (SRBGR) for Wireless Sensor Networks', PloS ONE, vol. 12, no.1.

3. Anju, S, Kingsly, SR &Patra, PSK 2014, 'A Secured Load Balanced Clustering Algorithm for Wireless Sensor Network', International Journal of Research in Computer and Communication Technology, vol. 3, pp. 517-520

4. Ankit, T &Ketan, K 2014, 'Cluster Head Election for Energy and Delay Constraint Applications of Wireless Sensor Network', IEEE Sensors Journal, vol. 14, no. 8, pp. 2658-266.

5. Ari, AAA, Blaise, OY, Nabila, L, Irepran, D &Abdelhak, G 2015, 'A power efficient cluster-based routing algorithm for wireless sensor networks: Honeybees swarm intelligence based approach', Journal of Network and Computer Applications, vol. 69, pp. 77-97.

6. Hart, JK & Martinez, K 2006, 'Environmental Sensor Networks: A revolution in the earth system science', Earth Science Reviews.

7. Heinzelman, WR, Chandrakasan, A &Balakrishnan, H Jan 2000, 'Energy- efficient communication protocol for wireless microsensor networks, Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS-33), pp. 3005-3014.

8. Heinzelman, WR, Chandrakasan, A &Balakrishnan, H 2020, 'An application specific protocol architecture for wireless microsensor networks', IEEE Transaction on wireless communication, vol. 1, no. 4, pp. 660-670.

9. Hiren, KDS, Rajib, M &Avijit, K 2016, 'E2R2: Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks', IEEE Systems Journal, vol. 10, no. 2, pp. 604-616.

10. Ibriq, J &Mahgoub, I 2006,‘ Asecure hierarchical routing protocol for wireless sensor network’, Proceedings of IEEE International Conference on Communication Systems, pp. 1-6.

11. Jiang, CJ, Shi, WR, Tang, XL, Wang, P & Xiang, M 2012, ‘Energy balanced unequal Clustering protocol for wireless sensor networks’, Journal of software, vol. 23, no. 5, pp. 1222-1232

12. Johnson, DB &Maltz, DA 1996, ‘Dynamic Source Routing In Ad Hoc Wireless Networks’, in Mobile Computing. Norwell, MA, USA: Kluwer Publishers, pp. 153-181.

13. Jothi, M, Ganapathy, S & Kannan, A2016, ‘Intelligent Data Gathering and Energy Efficient Routing Algorithm for Mobile Wireless Sensor Networks’, Asian Journal of Information Technology, vol.15, no.5, pp. 921-927.

14. Juan, L, Jinyu, H, Di W &Renfa, L 2015, ‘Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks’, IEEE Transactions on Industrial Informatics, vol. 11, no. 1, pp. 112-121.

15. Junfeng, W, Zhang, Y,Jialun, W& Chen, M 2015,‘PWDGR:Pair-Wise Directional Geographical Routing Based on Wireless Sensor Network’, IEEE Internet Of Things Journal, vol. 2, no. 1, pp. 14-22.

16. Kulothungan, K, Ganapathy, S, IndraGandhi, S, Yogesh, P & Kannan, A 2011, ‘Intelligent secured fault tolerant routing in wireless sensor networks using clustering approach’, International Journal of Soft Computing, vol. 6, no.5, pp. 210-215.

17. Leu, JS, Chiang, TH, Yu, MC & Su, KW 2015 ‘Energy Efficient Clustering Scheme for Prolonging the Lifetime of Wireless Sensor Network With Isolated Nodes’, IEEE Communications Letters, vol. 19, no.2, pp. 259-262.

18. Li, F, Zhang, B & Zheng, J 2011, ‘Geographic hole-by passing forwarding protocol for wireless sensor networks, ’IET Communication., vol. 5, no. 6, pp. 737-744.

19. Li, J, Jannotti, J, De Couto, DS, Karger, DR& Morris, R 2000, ‘A scalable location service for geographic ad hoc routing’, Proceedings of the 6th annual international conference on

Mobile computing and networking, pp. 120-130.

20. Lindsey, S &Raghavendra, CS 2020, 'PEGASIS: Power-efficient gathering in sensor information system', Proceedings of the IEEE Aerospace conference, vol. 3, pp. 1125-1130.

21. Li, X, Jia, Z, Zhang, R & Wang, H 2010, 'Trust based on demand Multipath routing in Mobile Ad Hoc Networks', IET Information Security, vol. 4, no. 4, pp. 212-232.

22. Logambigai, R & Kannan, A 2015, 'Fuzzy logic based unequal clustering for wireless sensor network', Wireless Networks, Springer, pp. 1-13.

23. Logambigai, R & Kannan, A 2016, 'Fuzzy logic based unequal clustering for Wireless Sensor Networks', Wireless Networks, vol. 22, no.3, pp. 945-957.

24. Logambigai, R, Ganapathy, S & Kannan, A 2016, 'Cluster Based Routing With Isolated Nodes in WSN', International Journal for Research in Applied Science & Engineering Technology, vol. 4, no.3, pp. 343-346.

25. Manjeswar, A & Agrawal, DP 2001, 'TEEN: A routing protocol for enhanced efficiency in wireless sensor networks', Proceedings of the IEEE Parallel and Distributed Processing Symposium (IPDPS), SanFrancisco, USA, pp. 2009-2015.

26. Manjeswar, A & Agrawal, DP 2020, 'APTEEN: A hybrid Protocol for efficient routing comprehensive information retrieval in wireless sensor networks', Proceedings of the IEEE Parallel and Distributed Processing Symposium (IPDPS), Florida, USA, vol. 2, pp. 195-202.

27. Mhatre, V & Rosenberg, C 2004, 'Homogeneous vs Heterogeneous clustered sensor networks: a comparative study', Proceedings of IEEE International Conference on communications (ICC), Paris, France, vol. 6, pp. 3646-3651.

28. Mohammad, S &Jalali, A 2017, 'Optimized sugeno fuzzy clustering algorithm for wireless sensor networks', Engineering Applications of Artificial Intelligence, vol. 60, pp. 16-25.Muhammad, A & Tae, HC 2016, 'Energy efficient fuzzy adaptive selection of verification nodes in wireless sensor networks', Ad Hoc Networks, vol. 47, pp. 16-25.

29. Padmalaya, N & Anurag, D 2016, 'A Fuzzy Logic-Based Clustering Algorithm for WSN to Extend the Network Lifetime', IEEE Sensors Journal, vol. 16, no. 1, pp. 137-144.

Perkins, C & Royer, E 1999, 'Ad Hoc On Demand Distance Vector Routing', in Proceedings 2nd IEEE Workshop Mobile Computer System Application, pp. 90–100.