European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 3, 2020

WSN Protocols, Research challenges in WSN, Integrated areas of sensor networks, security attacks in WSN

Vandana Saini[1], Jatin Gupta[2], Kamal Deep Garg[3]

[1]*Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*
[2]*Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*
[3]*Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*

[1]vandana.s@chitkara.edu.in, [2]jatin.gupta@chitkara.edu.in, [3]kamaldeep.garg@chitkara.edu.in

Abstract: Wireless Sensor Networks (WSNs) are widely used nowadays for seamless data transfer from one sensor node to others using the wireless channel. The term routing means sending the data packets from a source node to the destination node. There exist various routing protocols that ensure the efficient delivery of data from source to destination in terms of distance, energy and Received Signal Strength Indicator etc. In this paper various WSN routing protocols are reviewed to identify gap in study.

Keywords: WSN, Routing, Security, Attack, energy

1. Review of existing literature on Routing Protocols in WSN

There exist many routing protocols in which route the data packets on the basis of many factors like strength, energy, shortest path etc. Some routing protocols are discussed below and also to brief the study routing protocols are discussed in table 1.

1.1 Region Source Routing Protocol (RSRP)

A region-based energy-efficient source routing protocol elects the source nodes dynamically from all the regions based on the higher energy [1]. In this work, the author used an ant colony optimization scheme to find the most optimal source node from the region. The nodes were optimally selected based on an initialized population where the goal is to find the optimal solution at every iteration. The proposed algorithm had shown better outcomes in contrast with various existing algorithms in terms of lifetime, packet delivery ratio, delay and load.

1.2 Improved Energy Efficient- Low Energy Adaptive Clustering Hierarchy (IEE-LEACH)

IEE-LEACH selects the cluster head (CH) nodes based on residual and the average network energy instead of electing CH directly on a rotation basis. The threshold value is also computed in every round to select the data forwarding as single or multiple hops. The selection of CH ensures the data delivery to a base station as the elected CH has the highest residual energy. IEE-LEACH significantly reduces energy consumption as well as overall global cost [2].

1.3 Threshold Sensitive Energy Efficient Sensor Network (TSEP)

TSEP is one of the clustering-based energy-efficient routing protocols used to reduce energy consumption and to improve the network lifetime. In TSEP, the various levels of heterogeneity were defined among the nodes. The advance heterogeneity level contains the

nodes with the highest residual energy followed by intermediate and normal level of heterogeneity. The nodes at higher level can move to a lower level based on energy. The nodes in a lower level of heterogeneity perform minimum operations of data transfer, whereas the entire load is on an advance level to balance the nodes lifetime. TSEP had shown the enhance network lifetime and maintain the balance between alive and dead nodes.

1.4 Energy Efficient Clustering- Shortest Path Routing Protocol (EECSRP)

EECSRP selects the shortest routing paths to transfer the data from CH to base station. The protocol uses a sensing mechanism where the regions with homogeneous low energy nodes were set to distribute across the network to avoid the formation of sink holes. The nodes once distributed across the network, the transfer distance among the nodes decreases as low energy nodes never selected as CH. So, the data is transferred using single hop to CH. EECSRP had shown better results for network throughput, delay and energy [3].

Table I represents the comparison of routing protocols for WSN on the basis of different parameters like delay, network lifetime and load, energy Consumption and many more.

Table I Comparison Study of Routing Protocols in WSN

Protocol	Methodology	Performance Parameters	Merits	Simulator Used	Network Type
WECRR [4]	Learning-based clustering with a dynamic cost function for CH selection	Delay, Network Lifetime and Load	Drop free Efficient and reliable end to end delivery	Network Simulator-2	Homogeneous
K-CHRA [5]	Region CH selection with the integration of mixed-integer approach	PDR and Energy Consumption	Enhance network lifetime with balance energy consumption	OMNET++	Heterogeneous
CL-LEACH [1]	Residual Energy and Distance-Based CH selection	ALIVE Nodes, Energy Dissipation and Global Cost	Better Network Lifetime	Network Simulator-2.34	Homogeneous
CREEP [6]	The threshold-based fractional calculation for CH selection	Throughput and Network Lifetime for Mobile and Static Nodes	Reduced complexity due to restriction on elected CH numbers	MATLAB-2018	Homogeneous
MFABC [7]	CH selection based on modified adaptive threshold function elected based on the region to BS ration. Elected CH send data after aggregation to reduce the transfer load	Alive Nodes and Dead Nodes	Maximize the lifetime for nodes in all the regions, achieving uniform dead node graph	MATLAB	Homogeneous
PBCCP [8]	CH was elected based on PSO genetic algorithm. At each iteration, the network will find the most optimal solution to select CH at every round.	PDR, Energy Consumption and Delay	Support network scalability up to 1500 sensing nodes Energy-efficient Routing	NITTS	Homogeneous

CARP [9]	Cuckoo search optimization algorithm for CH selection. Intelligent and adaptive parameters based CH selection.	First Alive and Dead Node Round Optimization Ratio and Energy Consumption	Dynamic CH selection Lesser Drop Rate and Overheads Higher aggregation ration to enhance network lifetime	MATLAB-2018	Homogeneous
ABR [10]	Balanced Energy Consumption with CH selection on a hybrid method. CH elected based on K-Mean and Genetic Algorithm	Residual Energy Throughput Load	Clusters were done using the K-Mean algorithm. Clusters contain nodes based on mean distance. Mobile Base Station reduces the transfer	Network Simulator-2	Homogeneous
PSOBS [11]	To enhance the network lifetime PSO algorithm used with the integration of algorithms K-Mean and Mobile Sink nodes	Energy Consumption Hop Count Throughput	Effective Management of all the available network resources as a sink is mobile so CH efficient selection not required	MATLAB-2017	Homogeneous
HEEMP [12]	The CH nodes were selected on a centralized based scheme to reduce the energy consumption, where the parameters were computed for complete network	Scalability Alive and Dead Nodes Energy Consumption	The scalability of the network is much extendable and support more sensor nodes addition	MATLAB-2016	Homogeneous
CAMP [13]	Method stress on uniform energy depletion. Intelligent CH selection for all the created virtual zones	Converge Ratio Energy Consumption Dead Nodes	Improved Network Lifetime	MATLAB	Homogeneous
HMR WSN [14]	To improve QoS and throughput nodes are selected as CH based on Euclidian Distance	Packet Loss End to End Delay Overheads	Multipath Routing Collision Avoidance Enhance Lifetime	Network Simulator-3	Homogeneous

2. Security Attacks in Wireless Sensor Networks

Sensor nodes use broadcast transmission medium. Therefore, WSN are more susceptible to security attacks. An attacker can easily attack on the sensor networks, as nodes were deployed in a hostile environment. Attacking classes are mainly of two types (1) based on the location of an attacker and (2) based on the strength of an attacker as depicted in Figure 1.

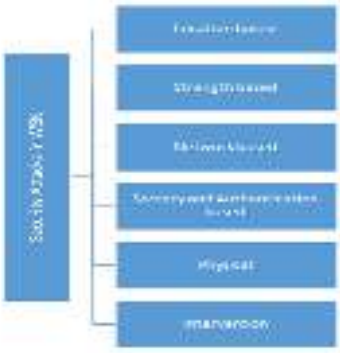

Figure 1: Classification of Security Attacks in WSN

2.1 Attacks Based on the Location of an Attacker.

Attacks can be either internal or external. Internal attack refers to an attack created by any genuine node in the network. External attack refers to an attack created by an external entity.

i. **Internal Attacks: An** attack is considered as an internal attack if any genuine node of the network acts abnormally. An attacker can compromise any legitimate node. An attacker can physically capture the node and obtain its secret key material [15].
ii. **External Attacks**: An attack is considered as an external attack if an external node performs it. In this case, an attacker does not have any cryptographic information or any internal network information.
iii. **Passive Attacks**: Passive attacks do not disturb the communication between nodes. The goal of an attacker is to monitor packets exchanged within wireless sensor networks. Eavesdropping is also a kind of passive attack. For draining the receiver's battery, an attacker can inject useless packets. The goal of an attacker is to run some malicious code and disturbs the normal functionality of the network.
iv. **Active Attacks**: An active attacker can do traffic monitoring, traffic analysis, information interruption and modification. Active attacks disturb normal communication between nodes. Example of active attacks includes denial of service, jamming, message replay and impersonating [16].

2.2 Attacks Based on Attacker's Strength.

Devices used by an attacker may have high capabilities in terms of antenna and computation power under two categories: (1) laptop class attacker and (2) mote class attacker.

i. **Laptop Class**: This type of attacker may have powerful devices such as high power radio transmitter, large battery power, faster CPU and bigger memory space. The goal of an attacker is to run malicious code and disturb the normal functionality of the network. The attacker may try to steal the secret cryptographic material from the sensor node.
ii. **Remote Class:** Remote class attackers have the same capabilities as the sensor nodes. Attackers obtain access to one or more sensor nodes for launching an attack. The goal of an attacker is to disturb the network using only the capabilities of a sensor node. Therefore, these types of attacks are limited [17].

2.3 Physical Attacks in WSN

Tampering refers to a modification of the internal structure of a single chip. Physical attack refers to direct physical access to the sensor node [18]. Depending on the effort, physical attacks were categorized into three types:

i. **Easy Attacks**: These types of attacks can be mounted quickly and with cheap equipment. It influences sensor readings. The attacker has access to the memory of the sensor node.
ii. **Medium Attacks**: These attacks require preparing non-standard laboratory equipment outside the sensor field. An attacker can access the RAM of the microcontroller and flash memory. The goal of an attacker is to access cryptographic keys.
iii. **Hard Attacks:** These attacks require non-standard laboratory equipment in the field. An attacker has access to the microcontroller for read/write. An attacker can analyze the program and change it as per needs.

2.4 Intervention in WSN

It indicates what an attacker can do. Different types of attackers are described as below [19]:

i. **Eavesdrop**: An attacker can only listen to network traffic and analyze it, but no action performed by the attacker. This attack is difficult to detect as it is a silent attack.
ii. **Crashing:** An attacker can destroy sensor nodes. An attacker attacks such that the sensor nodes completely break down.
iii. **Disturbing:** An attacker can upset the sensor node by measuring fake data. An attacker can selectively jam the network by disturbing the routing table. This results in data collisions which further lead to packet drop.
iv. **Limited Passive:** An attacker can open the node and use its secret material like Mac, IP and other parameters. Based on which an attacker can create an identity theft attack. The other node starts to send data to that malicious node which results in jamming or packets drop.
v. **Passive:** An attacker can steal the secret material of the node. An attacker can modify the node's data. This attack is very difficult to detect as it is a silent attack. The modified information when forwarded to the other network nodes may results in paralyzing the network completely.

2.5 Type of Network Attacks on WSNs

1. **Sinkhole Attack**: The attacker's goal is to attract traffic from a particular area through a compromised node. The attacker node was equipped with powerful hardware. A compromised node looks attractive with respect to routing algorithm, and it is placed near to the sink node or placed such that it covers the whole part of the network [20].
2. **Black hole Attack:** An attacker falsely advertise good path. To establish the path from source to the destination, the source node broadcasts route request packet to the neighboring nodes. Every intermediate node broadcasts the route request packet to its neighbors. When the unauthorized node receives the route request packet, it immediately sends a route reply packet. In this way, the path was established from the source to the malicious node. The goal of an attacker is to drop all the packets.
3. **Byzantine Attack:** These types of attacks are challenging to detect. A set of malicious nodes work in collusion to create routing loops, selective dropping packets and forwarding packets in non-optimal routes [21].
4. **Selective Forwarding Attack:** An attacker forwards selective packets while dropping the remaining packets. An attacker can periodically drop certain packets or can drop packets coming from the certain node
5. **Sybil Attack:** A malicious node spoofs the identity of other legitimate nodes [22]. One node presents multiple identities simultaneously. Encryption and authentication mechanism can prevent an attacker from launching a Sybil attack. Sybil attack was avoided by using public-key cryptography, but it is too costly for resource-constrained wireless sensor nodes.

6. **Hello Flooding Attack**: Using high powered transmitter, the attacker node falsely broadcast that it has a shorter path to reach to the base station [23]. When the nodes receive the HELLO packets, they start to transmit. These nodes are not in the transmission range of the malicious node.
7. **Jamming**: A malicious entity interferes the frequencies of radio of WSNs for creating a jamming attack. A single malicious node can disable the entire network. The resistance to jamming attack is to use frequency hopping spread spectrum. As per the hopping sequence, communicating devices frequently hop between frequencies [22]
8. **Tempering:** Sensor nodes are unattended after deployment. Therefore, they are susceptible to physical attacks. An attacker can physically damage or modify the device for gaining access to cryptographic keys. The resistance to tampering is to use temper proof materials and a device deletes its information once an attack is detected.

2.6 Attacks on Secrecy and Authentication

Privacy preservation in a WSN is a challenging issue. The attacker systematically monitors the traffic and derives sensitive information. Following are some attacks on sensor data privacy [23]:

1. **Eavesdropping and Passive Monitoring:** If the cryptographic mechanism was not applied to the messages, an attacker could easily understand it. An adversary can eavesdrop and passively monitors the messages.
2. **Traffic Analysis:** Through traffic analysis, an adversary can identify some nodes whose role is special. An adversary can also identify the activities and events in wireless sensor networks.

3. Research Challenges in Wireless Sensor Networks

Wireless Sensor Networks uses air as a medium to transfer data from one wireless node to others. Using WSN involves many challenges as below:

1. **Power Management:** The wireless sensor nodes are battery operated nodes and had limited power due to which the wireless nodes energy deplete after some time and node become dead. The major goal of various authors is to reduce the energy consumption of the wireless nodes to enhance the network lifetime. The power of sensor nodes is still a challenging issue, as it requires a never-ending improvement [2].
2. **Topology Issues:** The topology of WSN was not fixed as nodes are mobile in nature. The nodes are moving from one position to other, which results in a change of topology after every transmission round. The changing topology may degrade the network performance as during the data transfer if the network topology change then the respective distance between source and destination may be increased results in more energy consumption [3].
3. **Security Attacks:** Wireless networks are much prone to various security attacks due to their openness. Under various attacks, network performance starts to degrade, so it is very to detect and recover the network from attack to withstand the network performance. Still, to immune the network from various security attacks is a big issue to address. Even there exist many security protocols that guarantee to detect and recover network from attack. Still, no protocol ensure complete network protection [24], [25].
4. **Network Coverage:** The boundaries of the wireless sensor network were not fixed; the strength of the signal may vary from position to position. The goal is to design a WSN which guarantee complete network coverage with no blocking point as it degrades the network performance. The nodes in or near block points may drop data packets due to no network connectivity. So, it is one of the open question to design a WSN which ensure complete network coverage.
5. **Other Issues:** Hardware, Deployment, Medium Access Control, Architecture, Data Aggregation [26]

4. WSN Integrated Areas

WSN is one of the revolving fields due to its numerous applications and integrated areas. WSNs can be integrated almost in all the fields, some of the major area of integration are discussed below:

1. **Software-Defined Networks:** WSNs are integrated with software-defined networks to make them more robust. The sensor devices could be deployed in a way that they are used to acquire the information for the network based on which the paths can be defined [27].
2. **Internet of Things Network and Devices:** IOTs were used in many fields like communication, agriculture, health and surveillance. IoT based WSNs are used in all such fields to monitor the environment and fetch real-time data. The sensors were used to send all information to the base station [18].
3. **Computer Vision:** The WSNs can also be used and integrated into the field of computer vision. There were various application of computer vision like intelligent traffic and flood control where the real-time photographs are capture to acquire real-time information. But only acquiring the real-time data is of no use if the information cannot be given to action authorities in time. The sensor nodes were used to fetch such information and send the information over to the server using wireless channel [28], [29].
4. **Self-Driving Cars:** The self-driving cars use many sensors to monitor the environment and surroundings dynamically. The sensor network captures the data and pass to the learning models for real time decision making.
5. **Natural Language Process:** WSN are widely integrated in the field of language processing to acquire the different type of inputs like audio, speech and sign language. The NLP system are dependent on WSN to collect the data for processing as well as to transmit data with defined action or output to the user or input.

References

[1] C. Xu, Z. Xiong, G. Zhao, and S. Yu, "An energy-efficient region source routing protocol for lifetime maximization in WSN," *IEEE Access*, vol. 7, pp. 135277–135289, 2019.

[2] Y. Liu, Q. Wu, T. Zhao, Y. Tie, F. Bai, and M. Jin, "An improved energy-efficient routing protocol for wireless sensor networks," *Sensors (Switzerland)*, vol. 19, no. 20, pp. 1–20, 2019.

[3] M. Inam, Z. Li, Z. A. L. I. Zardari, and F. M. Mohammed, "Energy Efficient Clustering and Shortest-Path Routing Protocol (EECSRP) in Wireless Sensor Networks," in *International Symposium on Advanced Networks and Telecommunication Systems, ANTS*, 2019, no. December.

[4] K. Haseeb and K. Abu, "WECRR : Weighted Energy-Efficient Clustering with Robust Routing for Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 45, no. 5, pp. 1–23, 2017.

[5] Z. Wei *et al.*, "K-CHRA : A Clustering Hierarchical Routing Algorithm for Wireless Rechargeable Sensor Networks," *IEEE Access*, vol. 7, no. November, pp. 81859–81874, 2019.

[6] X. Zhao, S. Ren, H. Quan, and Q. Gao, "Routing protocol for heterogeneous wireless sensor networks based on a modified grey wolf optimizer," *Sensors (Switzerland)*, vol. 20, no. 3, pp. 1–18, 2020.

[7] P. Maratha and K. Gupta, "A comprehensive and systematized review of energy-efficient

routing protocols in wireless sensor networks," *Int. J. Comput. Appl.*, vol. 54, no. 3, pp. 1–18, 2019.

[8] A. Pathak, "A Proficient Bee Colony-Clustering Protocol to Prolong," *J. Comput. Networks Commun. Vol.*, vol. 32, no. 8, pp. 1–9, 2020.

[9] M. Faheem and R. A. Butt, "QoSRP : A Cross-Layer QoS Channel-Aware Routing," *Sensors*, vol. 21, no. September, pp. 1–36, 2019.

[10] S. Liu, Y. Yang, and W. Wang, "Research of AODV Routing Protocol for Ad Hoc Networks," in *AASRI Conference on Parallel and Distributed Computing and Systems Research*, 2018, vol. 5, pp. 21–31.

[11] S. Tabibi and A. Ghaffari, "Energy - Efficient Routing Mechanism for Mobile Sink in Wireless Sensor Networks Using Particle Swarm Optimization Algorithm," *Wirel. Pers. Commun.*, no. September, pp. 1–15, 2018.

[12] N. Malgotra, N. Mittal, and P. Singh, "A Hybrid Energy Efficient Reactive Multipath Routing for Wireless Sensor Network," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 9, pp. 211–217, 2019.

[13] A. Shukla, "A multi-tier based clustering framework for scalable and energy efficient WSN-assisted IoT network," *Wirel. Networks*, vol. 4, no. February, 2020.

[14] H. Jadidoleslamy, "A Hierarchical Multipath Routing Protocol in Clustered," *Wirel. Pers. Commun.*, vol. 34, no. 5, pp. 1–20, 2017.

[15] I. Butun, P. Osterberg, H. Song, and S. Member, "Security of the Internet of Things : Vulnerabilities , Attacks and Countermeasures," *IEEE Commun. Surv. TUTORIALS*, vol. 65, no. 11, pp. 1–25, 2019.

[16] M. A. Elsadig, A. Altigani, M. Abuelaila, and A. Baraka, "Security Issues and Challenges on Wireless Sensor Networks," *Int. J. Adv. Trends Comput. Sci.*, vol. 8, no. 4, 2019.

[17] P. Sharma and M. Sharma, "Threshold Based Algorithm for the Detection of DDOS Attack in Wireless Sensor Networks," *Int. J. Recent Technol. Eng.*, vol. 8, no. 4, pp. 1869–1873, 2019.

[18] K. Lounis, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," *IEEE Access*, vol. 8, no. May, 2020.

[19] J. Mo and H. Chen, "A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks," vol. 2019, 2019.

[20] U. Ghugar and J. Pradhan, "A Review on Wormhole Attacks in Wireless Sensor Networks," no. June, 2019.

[21] H. Lin *et al.*, "Minimum Byzantine Effort for Blinding Distributed Detection in Wireless Sensor Networks," *IEEE Trans. Signal Process.*, vol. 43, no. 4, p. 1, 2020.

[22] S. Boyuan and L. Donghui, "A Reputation-Based Method against Combinations of Internal Attacks in WSNs," pp. 2251–2255, 2016.

[23] O. Almomani, "An Anonymous Channel Categorization Scheme of Edge Nodes to Detect Jamming Attacks in Wireless Sensor Networks," pp. 1–19.

[24] A. Somauroo and V. Bassoo, "Energy-efficient genetic algorithm variants of PEGASIS for

3D Wireless Sensor Networks," *Appl. Comput. Informatics*, vol. 34, no. 7, pp. 1–23, 2019.

[25] L. Tang, Z. Lu, and B. Fan, "Energy efficient and reliable routing algorithm for wireless sensors networks," *Appl. Sci.*, vol. 10, no. 5, 2020.

[26] M. M. Warrier and A. Kumar, "An Energy Efficient Approach for Routing in Wireless Sensor Networks," *Procedia Technol.*, vol. 25, no. Raerest, pp. 520–527, 2016.

[27] M. Abujubbeh, F. Al-turjman, and M. Fahrioglu, "Software-defined wireless sensor networks in smart grids : An overview," vol. 51, no. August, 2019.

[28] A. H. Allam, M. Taha, and H. H. Zayed, "Enhanced Zone-Based Energy Aware Data Collection Protocol for WSNs (E-ZEAL)," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 21, no. 5, pp. 1–11, 2019.

[29] J. Yun and M. Kim, "SybilEye : Observer-Assisted Privacy-Preserving Sybil Attack Detection on Mobile Crowdsensing," 2020.