THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Comparative Study on Attacks of Routing Protocols In Wireless Sensor Networks

Mohit Singh Bisht[1], Arvind Kumar[2]

[1]Research Scholar, School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India
Email: bisht.mohit604@gmail.com

[2]Assistant Professor, School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab,India
Email: arvind28april@gmail.com

Abstract: Wireless sensor network is the part of ad-hoc network which is self-adaptive, self-healing, decentralized, dynamic topology and limited power consumption. These wireless sensor network means no wired connection used in emergency services like military, hospitals, universities, etc. They all are using small sensors which are deploying in a particular region in a limited range because of these pros, sensors have the capability to change their mobility via this application used in WSNs able to communicate end to end host in a wireless network. In this paper, these wireless networks having the routing protocols like DSDV, AODV etc. have the capability to remove the congestion and forward the data packet from one node to another node.

Keywords: WSN, LEACH, AODV, DSR, PEGASIS, routing protocols.

1. INTRODUCTION:

Wireless Sensor Network is famous as most significant innovation in twenty-first century. A wireless sensor network works from huge number of sensor hubs that unite themselves to frame a wireless network. Routing in WSNs is exceptionally testing from other wireless networks since WSs are small size devices equipped with radio transceivers and low power batteries [1]. WSN are utilized for some applications, for example, flood location, home mechanization, natural checking, woods fire discovery and so forth. Due to the potentially harsh, unpredictable environments in which sensor networks are expected to work, apart from the energy and the bandwidth constraints, sensor networks pose several technical challenges to the researchers. The wireless sensor networks must deal with limited resources that are often dynamically changing. The network also needs to deal with unreliable communication links that are easily affected by interference, and yet it should provide the required reliability. Different routing protocols are accessible to build the lifetime of network. for increasing the lifespan of network, there are various types of routing protocols. Networks are split into different types of clusters in this system [2]. Single node is classified as a cluster head (CH) in each cluster and non-cluster head nodes are treated as individuals in the cluster. In each cluster, cluster head accumulates the information from the cluster individuals and total this information and communicate this information to Base station through single-path or multi-path. CHs use more vitality than the CM [3].

WSN routing protocols are important for the discovery and maintenance of power-efficient paths to ensure dependable communication. In WSN routing protocols are categorized into two types: Based on network structure and path establishment.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

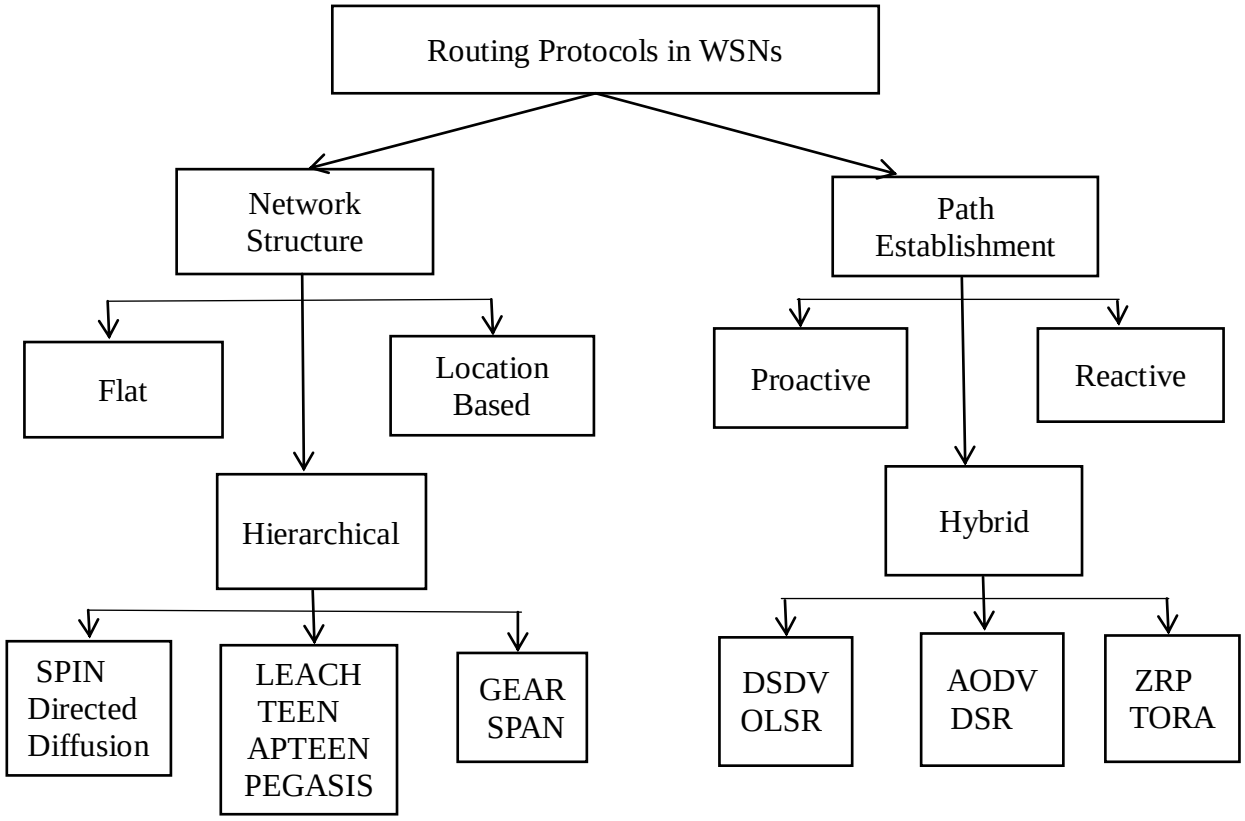

Figure 1: RoutingProtocols in Wireless Sensor Networks

1) **Network structure:** It is divided into three parts:

   i. **Flat routing protocol:** It is a protocol for device correspondence performed by switches in which all switches are the companions of each other. The flat routing protocol disperses data routing to switches that are connected to each other without any framework of connection or separation between them.

   ii. **Hierarchical based routing protocol:** It is used to route the traffic from source to the destination via Cluster Head (CH). This sort of routing convention sub-partition the WSN into small clusters and build a hierarchy of nodes. it is a feasible solution to reduce power usage in WSNs due to decreased unnecessary transfer of data.

   iii. **Location based routing protocol:** It is utilized in WSN, in which the data about the location of nodes is utilized for correspondence. It is otherwise referred to as routing protocols based on geographic routing or position

2) **Path Establishment:** It is categories into three types:

   i. **Proactive:** In a proactive routing protocol, each node keeps up at least one tables speaking to the whole topology of the system. These tables are refreshed consistently so as to keep up exceptional routing data from every node to each other node.

   ii. **Reactive:** It recognized as rules on request as it makes routes at the point at which

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

they are required, as it were. The need begins with the source, which starts a process of disclosing the route within the system. Once a route has been identified or all possible path modifications have been evaluated, this process is fulfilled. After that the process of path maintenance takes place to retain the valid paths and eliminate the incorrect paths.

iii. **Hybrid:** It is combination of both proactive as well as reactive routing protocol. in this process network splits into zones for routing. this protocol is also known as Zone Routing Protocol.

1.1. Advantages of WSNs:

- **Flexible:** WSN is an adaptable system and can adjust to the changes. On the off chance that there is an irregular sort circumstance happen, that time we will require an extra workstation.
- **Additional of new device:** WSN can suit new gadgets in the system whenever easily.
- **Save Cost:** Wireless sensor systems spare a great deal of wiring cost and sensors like PIR (latent infrared) identifiers are generally less expensive at that point wires.
- **Useful to society:** Organizing wireless sensors are used in a kind of fields such as medical services, protection, environmental monitoring which benefits human well-being.

1.2. Disadvantages of WSNs:

- **Security:** WSN systems are not or less secure when contrasted with wired systems. Hackers can easily hack the network because hacker’s laptop can be act as access point.
- **The problem of the battery:** Nodes should be charged at regular intervals. The node's battery life is exceptionally short.
- **Complexity:** Complexity is more to configure as compare to wired network.
- **Distraction:** Wireless sensor systems continue diverting by different remote gadgets.

1.3. Applications of WSNs:

- **Environmental Monitoring:** It will be used as soon as possible as one of the sensor systems. Sensors are used in this process to observe a range of natural variables.
    - **Risk Observing:** Sensors can be utilized in areas such as a substance plant or a battle zone to screen for organic or chemical hazards.
    - **Habitation:** Sensors can be utilized to screen wild creature or plant states in wild living spaces, just like the environment's natural parameters.
    - **Disaster Monitoring:** In a planned district, sensors can be thickly sent to differentiate between common or non-natural events. For example, to identify timberland fires or floods, sensors can be dissolved in forest area or rescue oparation. In a structure, seismic

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

sensors can be used to determine the bearing and magnitude of a quake and to assess building safety.

- **Water or Air Quality Checking:** Sensors can be appropriated superficially or submerged to screen the standard of air and water. Such as, water perception can be utilized in the hydro-science field. Control of air standard can be utilized to handle the air pollution[4].

- **Health Maintenance:** Wireless sensor network can be utilized to screen and way older people and victims for medical services reasons, which can alleviate the serious deficiency of the workforce of social insurance and reduce the use of human services in the current framework for human services.

  - **Behaviour Monitoring:** Sensors can be transmitted to screen the patient's practices in a patient's home. For example, when the patient falls, it can caution specialists and requires prompt consideration for restoration. It can screen what a patient is doing and provide a TV or radio with updates or guidelines.

  - **Health surveillance:** Wireless sensors can be unified into a remote body region system to screen essential signs, natural parameters and topographical areas, allowing long-term, non-invasive and wandering inspections of patients or older people with temporary alarms for human services.

- **Militant Approach :** Wireless sensor networks are occuring a vital part of the framework of militant order, control, correspondence, and insight. Wireless sensors can be sent without foundation to a battle zone or unfriendly area.

  - **Battleground Monitoring**: Sensors can be sent to a battleground to monitor the proximity of resources and weapons and track their evolution in order to closely monitor opposing forces [5].

  - **Universal remote controling:** Sensors can be sent for remote detection, identification and observation of potential terrorist attacks on nuclear, natural and chemical weapons.

  - **Knowledgeable informing:** Sensors can be mounted on unmanned mechanical tanks, automobiles, military aircraft, ships, missiles in order to deal with obstacles to their targets and to encourage more effective assaults or guards.

- **Surveillance and Security:** Wireless sensor networks can also be utilized in numerous security applications, observation. Such as, video, acoustic, and various sensor types can be transmitted in structures, aircraft terminals, metros, and other basic foundations, such as nuclear power plants or correspondence focuses to recognize and follow interlopers, and provide convenient alerts and assurance from potential assaults. Not at all like applications that do not require a fixed foundation, many security applications can support setting up a power supply and correspondence framework [6].

- **Domestic Surveillance:** Wireless sensor networks can be utilized to assign people with progressively advantageous, intelligent living conditions.

  - **Bright Home:** WSs can be incorporated into a home and a self-ruling home network can be combined with structure. For example, a keen cooler associated with a smart stove or microwave can set up a menu depending on the stock of the refrigerator and send applicable cooking parameters to the shrewd stove or microwave, setting the ideal cooking time and temperature.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

- **Remote Metering:** WSs are utilized to view the utility meters in a house remotely, which includes electricity, water or gas and then transmit the measurements to a remote focus via transmission of wireless system [7].

1.4. Attacks in Wireless Sensor Networks:

1.4.1. Passive attacks: In Passive attacks, listening to the information of others going from one place to another and instructing them.This kind of attacks is simpler to acknowledge and it is difficult to detect. Since, the attacker does not make any change on traded data.

It is of two types

i. **Release of message content (Reading message content):** Important information on telephoning, emailing, sending a file, etc, is reliable information, in which unauthorized read messages occurring between two people who are attacking.

ii. **Observation of message pattern (see message pattern):** The Attacker sees the pattern of the message between two people unauthorized and misuses it.

1.4.2. Active attacks: Under active attack, the data has to be changed and misdirected, an attacker attempts to evacuate or change the messages transmitted on the networks.

It is divided into four parts:

i. **Masquerade:** It sends a user other unauthorized user messages, in place of another authorized user, which appears to be similar to the authorized user.

ii. **Replay:**In this, the unauthorized user captures the data unit with an authorized user and then stops it and generates unauthorized effects by sending it to another authorized user.

iii. **Modification in message:** Generally it means changing the message, sending it late, changing its sequence, so that it shows the wrong impression.

iv. **Denial of service:** This prevents the general use or management of communication services affects the efficiency of the entire network. This attack is either disabled to the network or the network is overloaded with the messages, so that the network does not work properly. And communication can be interrupted.

Active attacks are different from passive attacks, it is difficult to detect passive aggression but once it is detected, it is easier to stop them, while preventing active attacks is not easy.

1.5. Network Security:

Network security is a process. In this process we can save the networks by unauthorized access (without permission of access), hacking and denial of service attack, virus, worms etc. network security is not an easy task, it require experts.

we should monitoring of network for increasing the network security in any network,we should experiment of software and hardware components foe example firewall, antivirus software, intrusion detection system etc.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

1.5.1. Need of network security:

To protect the user's imported and confidential information from hackers and attackers in the internet. To Save Data and Information from Unauthorized Access, Loss and Modification.

1.5.2. Network security requirements:

i. **Confidentiality:** Confidentiality means that only the sender and the receiver can see or access the message.Confidentiality ends when a unautorized person accesses the message.

ii. **Authentication:** The authentication means authenticating the user's identity, meaning that the person has the message, that is the person who does not have any documents.

iii. **Integrity:** Integrity implies that there is no change in the message. In this process received data will remain unchanged, removed in transition by unauthorized nodes either by malicious attack or radio failure [8].

After sending the message of the message, any change can be possible in the message like Alter, Insert, Delete etc, then its Integrity ends.

iv. **Non-repudation:** Sometimes such a situation that when a user sends a message, but later he says that he didn't sent this message.

So non-repudiation does not consider such a kind of potentiality, i.e. non-repudiation, does not order to refuse after sending a message to Sender.

v. **Access Control:** Access control keeps track of what the user can access and which can not access.

vi. **Availability:** Availability says that the resource which will be available only for the authorized user, not the rest.

2. RELATED WORK:

Bakaraniya et al. [9] discussed a revised algorithm which is based on LEACH protocol. The revised protocol known as "Kmedoids-LEACH protocol for clustered WSN" is intended to extend the lifespan of the sensor networks by balancing the node's power consumption. The protocol used the clustering algorithm of kmedoids for uniform clustering and the use of euclidean distance and total residual energy for selecting the head of the cluster (CH).

Magotra et al. [10] proposed a non-cryptographic methodology for the discovery of HELLO flood attacks. There is a huge decrease in the occasions the test bundle is transmitted. The recreation results indicated that the quantity of test parcels sent for location was decreased from 20-35 to 10-14, a non-cryptographic answer for HELLO.

Yadav et al. [11] proposed the LEACH protocol to improve the performance of the Health Monitoring Network. They reduced the Mobile Health Monitoring power consumption and packet loss ratio so that Patient Health Record could be securely transferred. The execution of the LEACH Health Monitoring Network had been improved. They also reduced the Mobile Health Monitoring

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

ratio of packet loss and power Consumption so that Patient Health Record could be securely transferred.

Bengag et al. [12] proposed a WSN protocol called the APTEEN protocol to help improve the node's network existence by periodic monitoring of sensor nodes and communicating the appropriate parameters to farmers to take action. The nodes in such a network not only respond to time-critical situations, but also offer a very energy-efficient overall picture of the network at regular intervals. They also disscussed about the ant colony algorithm and home office based application.

Ghosh et al. [13] talked about the improved PEGASIS (E-PEGASIS) model which conquers the disadvantages and is energy efficient. The recreation results show that, comparative with PEGASIS, Binary PEGASIS and LBEERA, E-PEGASIS increases the lifespan of WSN along with a significant reduction in data latency. It is shown that the findings are statistically significant. They also talked about the ant colony optimization for data gathering.

Ullah et al. [14] presented a comparative analysis of clustering protocols based on HEED that were UHEED, HEED, and R-HEED variant that was ER-HEED. When considering different case studies, they found the similar model of network, the same model of power consumption and also compared the lifespan of the protocols. Their comparative study found that the choice of the procedure to be used depends on the case study and the calculation of the lifespan of the WSN considered.

Shendurkar et. al [15] discussed on the analysis of black hole attack on AODV routing protocol.In this attack, the malicious node delivers itself as having the shortest route by sending false routing response to all nodes.And it additionally improved the performance of various routing protocol.

Zhang et al. [16] presented a genetic algorithm bacterial exploring improvement calculation to play out the determination of the ideal directing. In the wake of looking out different courses to the goal hub, the ways were instated then the GA calculation was begun. This calculation rapidly finds the places of the greatest likelihood ideal ways, which was the underlying places of microscopic organisms for the bacteria foraging optimization calculation. Via utilizing the BFO calculation, it is anything but difficult to look out the outrageous worth and the ideal way so as to make up for the poor exactness of GA calculation. their proposed advanced procedure improved the directing choice calculation without change the unpredictability of DSR and demonstrates the union of the calculation to the worldwide ideal arrangement. The reenactment showed that the suggested calculation was probable and suitable and furthermore has better exploratory outcome.

Shivahare et al. [17] have driven audit of protocol properties of different MANET coordinating calculation and checked them. The routing counts considered are gathered into two classes proactive (table driven) and reactive (on demand). The calculation evaluated were DSDV, DSR, and AODV. The assessment between three routing protocol relied upon the diverse protocol property parameters, for instance, route Disclosure, System Overhead etc.

SreeRangaRajuet al.[18] suggested an algorithm to improve the efficiency of Zone Routing Protocol query control mechanisms for wireless ad hoc communications networks on metropolitan territory. Our proposed calculation improves the structure of the routing zone to give upgraded location and avoidance of covering inquiries. Such procedures can be implimented to single or numerous channel portable adhoc systems in order to enhance ZRP's delay and traffic control

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

efficiency. Their new algorithm enabled ZRP to include routes to all available network nodes, to less traffic control than exclusively proactive connection status or purely reactive path finding, and less time than traditional flood search.

Jing et al. [19] discussed the algorithm for routing based on the SPIN algorithm. Given the problem of "blindly forward" and "data unavailable" in SPIN, a current routing algorithm called SPIN-1 is suggested, simulated it with NS2 from two key elements: node energy usage and number of live nodes. The results indicate that not only the issues of blind forwarding and data availability were solved in SPIN, but also the power usage of the entire network was more homogenous.

Srivastav et al. [20] dissused while using the Geographical & Energy Aware Routing Protocol, emphasis was placed on the fact that the node commination should be energy-efficient by a smart neighbor selection to forward the packet to the sink. GEAR is a recursive information distribution scheme within the field. The group-based delivery model and the use of power-conscious routing make GEAR more efficient than the existing one. GEAR's routing design is based on two parameters: location and node levels of current and residual energy.

Table 1. Comparison of different routing protocols

Authors Name	**Year**	**Protocols**	**Algorithm Used**	**Attacks used in protocol**	**Application**	**Types**
Bakaraniya et al. [9]	2013	LEACH	k-medoids clustering algorithm	Jamming attack	Health monitoring	Hierarchical
Magotra et al. [10]	2014	LEACH	k-medoids clustering algorithm	Hello flood attack	Health monitoring	Hierarchical
Yadav et al. [11]	2017	LEACH	k-medoids clustering algorithm	Hello flood attack	Health monitoring	Hierarchical
Bengag et al. [12]	2018	TEEN / APTEEN	Ant colony algorithm	Black hole attack	Time critical / Home office	Hierarchical
Ghosh et al. [13]	2016	PEGASIS	Greedy algorithm/ Ant colony algorithm	Replica attack	Data gathering	
Ullah et al. [14]	2016	HEED	Iterative grouping algorithm	DOS attack	Energy efficient clustering	Hierarchical
Shendurkar et al. [15]	2014	AODV	RSA key generation algorithm	Black-hole attack	High traffic load or Zigbee	Reactive
Zhang et al.	2018	DSR	Genetic	Warm-hole	Mobile agent	Reactive

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

[16]			algorithm-bacterial foraging optimization	attack	-based appli-cation	
Shivahare et al. [17]	2012	DSDV	Bellman–Ford algorithm	Gray-hole at-tack	Visitor Tracking System	Proactive
SreeRangaRaju et al. [18]	2011	ZRP	Query control mechanisms	Black hole at-tack	Zigbee	Hybrid
Jing et al. [19]	2011	SPIN	Energy saving routing algorithm	Eavesdropping	Ecommerce ecosystem	Data centric
Srivastav et al. [20]	2015	GEAR	Recursive algo-rithm	Sybil attack	Home office or Gaming	Location based Protocols

3. CONCLUSION:

WSN over the past few years, plays a major role in enviormental scenario. These network setup in a flat and distributed infrastructure. They are used for monitoring the milatery targeting services, industrial areas, enviormental issues etc. They are used lot of algorithms to remove the issues of wireless sensor networks such as power consumption, limited bandwidth, limited frequency and dynamic topology. In this paper we have presented routing protocols consists hierarchical, location based, data centric and multi-path based. These are the rules which are followed by algorithm in wireless network. The algorithm such as Ant colony, k-medoids clustering, Bellman-ford etc. Via these algorithm able to take the shortest path between two nodes, forwarding the data packet. Routing protocols used in transport and application layer for forwarding the data packet from one process to another process. We are also presenting diffrences between the protocol with the help of some application, algorithm and attacks.

4. REFERENCES:

[1] E. Abdellah and S. Benalla, "Advanced Low Energy Adaptive Clustering Hierarchy," *Int. J. Comput. Sci. Eng. IJCSE*, vol. 02, no. 07, pp. 2491–2497, 2010.

[2] M. Aslam, N. Javaid, A. Rahim, U. Nazir, A. Bibi, and Z. A. Khan, "Survey of extended LEACH-based clustering routing protocols for wireless sensor networks," *Proc. 14th IEEE Int. Conf. High Perform. Comput. Commun. HPCC-2012 - 9th IEEE Int. Conf. Embed. Softw. Syst. ICESS-2012*, pp. 1232–1238, 2012.

[3] S. Sharma and S. K. Jena, "Cluster Based Multipath Routing Protocol for Wireless Sensor Networks," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 2, pp. 14–20, 2015.

[4] A. J. Whittle, M. Allen, A. Preis, and M. Iqbal, "Sensor networks for monitoring and control of water distribution systems," *Struct. Heal. Monit. Infrastruct. Sustain. - Proc. 6th Int. Conf. Struct. Heal. Monit. Intell. Infrastructure, SHMII 2013*, pp. 83–98, 2013.

[5] M. A. M. Vieira, C. N. Coelho, D. C. Da Silva, and J. M. Da Mata, "Survey on wireless sensor network devices," *IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA*, vol. 1, no. January, pp.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

537–544, 2003.

[6] M. Charalampidou, G. Pavlidis, and S. G. Mouroutsos, “Sensor analysis and selection for open space WSN security applications,” *Majlesi J. Electr. Eng.*, vol. 13, no. 1, pp. 95–108, 2019.

[7] W. Zhu, W. Qi, and H. Xiaoqiang, “The design of the remote water quality monitoring system based on WSN,” *Proc. - 5th Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM 2009*, pp. 1–4, 2009.

[8] G. Yang, L. Dai, G. Si, S. Wang, and S. Wang, “Challenges and Security Issues in Underwater Wireless Sensor Networks,” *Procedia Comput. Sci.*, vol. 147, pp. 210–216, 2019.

[9] P. Bakaraniya and S. Mehta, “K-LEACH: An improved LEACH Protocol for Lifetime Improvement in WSN,” *Ijettjournal.Org*, vol. 4, no. 5, pp. 1521–1526, 2013.

[10] S. Magotra and K. Kumar, “Detection of HELLO flood attack on LEACH protocol,” *Souvenir 2014 IEEE Int. Adv. Comput. Conf. IACC 2014*, no. February, pp. 193–198, 2014.

[11] D. Yadav and A. Tripathi, “Load balancing and position based adaptive clustering scheme for effective data communication in WBAN healthcare monitoring systems,” *Proc. 2017 11th Int. Conf. Intell. Syst. Control. ISCO 2017*, pp. 302–305, 2017.

[12] A. Bengag and M. El Boukhari, “Classification and comparison of routing protocols in VANETs,” *2018 Int. Conf. Intell. Syst. Comput. Vision, ISCV 2018*, vol. 2018-May, no. 1, pp. 1–8, 2018.

[13] S. Ghosh, S. Mondal, and U. Biswas, “Enhanced PEGASIS using ant colony optimization for data gathering in WSN,” *2016 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2016*, no. Icices, pp. 1–6, 2016.

[14] Z. Ullah, L. Mostarda, R. Gagliardi, D. Cacciagrano, and F. Corradini, “A comparison of HEED based clustering algorithms - Introducing ER-HEED,” *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 2016-May, no. March 2019, pp. 339–345, 2016.

[15] M. A. M.Shendurkar and N. R.Chopde, “A Review of Black Hole and Worm Hole Attack on AODV Routing Protocol in MANET,” *Int. J. Eng. Trends Technol.*, vol. 9, no. 8, pp. 394–399, 2014.

[16] D. gan Zhang, S. Liu, X. huan Liu, T. Zhang, and Y. ya Cui, “Novel dynamic source routing protocol (DSR) based on genetic algorithm-bacterial foraging optimization (GA-BFO),” *Int. J. Commun. Syst.*, vol. 31, no. 18, pp. 1–20, 2018.

[17] B. D. Shivahare, C. Wahi, and S. Shivhare, “Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol Property :,” *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 3, pp. 356–359, 2012.

[18] M. . SreeRangaRaju and J. Mungara, “Optimized ZRP for MANETs and its Applications,” *Int. J. Wirel. Mob. Networks*, vol. 3, no. 3, pp. 84–94, 2011.

[19] L. Jing, F. Liu, and Y. Li, “Energy saving routing algorithm based on SPIN protocol in WSN,”

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Proc. 2011 Int. Conf. Image Anal. Signal Process. IASP 2011, pp. 416–419, 2011.

[20] G. Srivastav, "Effective Sensory Communication using GEAR Protocol," *Int. J. Sci. Res.*, vol. 4, no. 5, pp. 1809–1815, 2015.