International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-10 Issue-1, May 2021

Wormhole Attacks in Wireless Sensor Networks (Wsn) & Internet of Things (IoT): A Review

Parvathy.K

***Abstract:** In the current world people are using the sensing networks called IoT and WSN as the subset of IoT in various applications. The employment of these sensor networks is rapidly increasing. Due to the longer usage of these sensor networks security issues are eventually happening and has the possibility of developing the attacks in the network. In this review, focuses on wormhole attacks in wireless sensor network (WSN) and Internet of Things (IoT) creating a tunnels i.e., wormhole link in between source and the destination node in the network. The classification of wormhole attack in both WSN and IoT are presented based on the mode of attacker. The detection mechanisms of wormhole attack are specified in both WSN and IoT. It hypothesizes the detection strength is more in IoT than the WSN based on the analysis, the parameters of the detection algorithm that the WSN is about 20% while in IoT is 70%.*

***Keywords:** Wireless Sensor Networks, Internet of Things, Security Attacks, Wormhole Attack.*

I. INTRODUCTION

A) Wireless Sensor Networks (WSN)

The Wireless Sensor Networks (WSN) which are group together to form sensor nodes by functioning these operations like signal processing, sensor configuration and computation [1]. These nodes which help to mitigate various application like environmental condition and application, military application, healthcare monitoring, habitat and industrial monitoring. The WSN is structured with sensor nodes, base station and the server [3]. The sensor nodes are connected to each other with base station and the server where the nodes are connected to the wireless medium for communicating to the sensor nodes, base station and the server [2]. The applications need to a large network with vast number of sensor nodes. Due to very limited usage of sensor nodes, there is the possibility of security issues that leads to insecure sate of network [29].

B) Internet of Things (IoT)

An Internet of Things (IoT) are the trending technology which arises day-by-day across the world along with the wireless communication. The IoT is formed by interconnecting many objects and the networks as physical objects as sensors and the network [3]. These devices are used everywhere in all over the area in vast number of applications.

Manuscript received on May 15, 2021.
Revised Manuscript received on May 20, 2021.
Manuscript published on May 30, 2021.
* Correspondence Author
Parvathy.K*, Assistant Professor, Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore (Tamil Nadu), India.

These applications can be in form smart objects as smart home, smart city, smart Agri, smart fitness, smart health etc [4]. The usage of IoT devices is mainly tracking, getting the information through sensors, capturing the data through sensors etc. For these process security issues are occurring more and thus result to insecure state of IoT devices [5].

C) Security Attacks in WSN and IoT

In WSN and IoT, the attacks are occurred during the communication between the devices by sending and receiving the data, Capturing the confidential information, tracking the details which is been monitored by a third party i.e., the intruder etc [2]. The attacks in WSN and IoT are categorized based on OSI layer models as in WSN the attacks are from Physical layer, datalink layer, network layer, presentation layer and application layer [3,29]. In IoT attacks are categorized as perception layer, network layer, middleware layer and application layer they are called IoT architectural layer attacks [4].

II. LITERATURE REVIEW

WSN and IoT are the sensor networks where the all devices are group together and used in wide range of applications.[5] discussion about the wormhole attack as Grave Attack, the attacker creates a place in the network to track the information from the network are represented. Classification of The attacks are discussed in different types as Half open wormhole, open wormhole and closed wormhole [2,4,6,7,8,29]. Illustration of different types of wormhole attacks that are explained as wormhole attack of IoT as Encapsulation, Out of Band Channel, High transmission power, Packet delay and Protocol Deviation [9,10,11,12]. The detection mechanisms of the wormhole attacks in IoT and WSN.each wormhole attacks in WSN are discussed. Geographic and temporal leashes [16,17] which help to detect using GPS algorithm. Approach discusses about lightweight process where the detection can be in quick and the packet loss [17]. identification of attack is represented in this approach by working under the principle by calculating the path time and predicted distance [18]. The illustrates the approach is also called as Location Aware Guard Node (LAGNs) [19]. The key establishment process took place in this approach for decoding the message. The approach is discussed about the performance wormhole attacks in found in multipath routing. The approach uses localization method to keep away from wormhole attack [20]. The approach uses watchdog and Delphi methods. In WSN this approach that provide information during the packet drop [21]. It is a unique method, where the data is received from the fingerprinting devices [20].

The method that can detect the wormhole attack with the help of directional antenna [21]. Discuss about various detection mechanisms of IoT [21]. The approach is to detect a wormhole attack in IoT [22]. The is AODV-HP (High-Performance Adhoc On-demand Distance Vector) routing protocol is a hybrid algorithm which is centered position [23]. The approach is attack-tolerant multi-path routing protocol where all the operation are performed in events like altering the paths, exchanging path information without additional communications [24]. The approach is used without any need of a hardware device and can also used in WSN [25]. The approach is a wireless network coding system called DAWN, this approach is a distributed detection algorithm [26]. The novel approach to improve the performance of the wireless sensor nodes by overcoming the exposure of AODV.These AODV have High Transmission Power type wormhole attack [27].

III. WORMHOLE ATTACK

Wormhole Attack is also called as Grave Attack, the attacker creates a place in the network to track the information from the network and get the confidential information from the users [5]. Fig 1 shows the wormhole attack where a tunnel or wormhole link is created in between source and destination. In between nodes of source and destination nodes are compromised nodes.

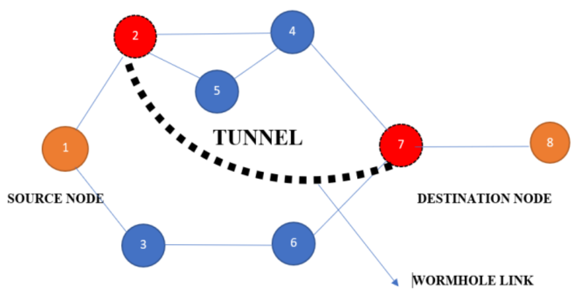

Fig.1.Wormhole Attack

Table.1. Wormhole Attacks in WSN and IoT

Wormhole Attack in WSN	Wormhole Attack in IoT
Half Open Wormhole Attack	Wormhole using Encapsulation
Open Wormhole Attack/Exposed Attack	Wormhole using Out of Band Channel
Closed Wormhole Attack/Hidden Attack	Wormhole using High transmission power
	Wormhole using Packet delay
	Wormhole using Protocol Deviation

A) Wormhole Attack in WSN

In WSN, the two nodes communicate among each other through a link those links are called as tunnel [2]. During the communication from source to destination, the attacker who get inside the two nodes and create a link i.e., tunnel. The Attacker who captures the packet from the tunnel and send a malicious node through the tunnel [7]. The Wormhole Attack in WSN are of three types: Open Wormhole Attack/Exposed, Half Open Wormhole Attack and Closed Wormhole Attack/Hidden. Table 1 shows the types of wormhole attack in WSN [8,29].

Half Open Wormhole Attack: In the source(S) node Malicious node M1 is visible, whereas M2 is set hidden. The tunnel path S-M1-D for the packets sent by S for D. In WSN, the attackers do not modify the data of the packet, by creating a tunnel the packet form one side of wormhole to another side [4].

Open Wormhole Attack/Exposed: The visible nodes are Source(S) and destination (D) nodes and wormhole ends M1 and M2. Nodes A and B are kept hidden on the traversed path. In this mode, a new procedure is introduced called route discovery procedure, where the attackers include themselves in the packet header. The malicious nodes are present and create a path so that direct neighbours in the network are in the malicious state [6].

Closed Wormhole Attack/Hidden: They keep hidden of all the intermediate nodes (M1, A, B, M2) on path from S to D. In this network both source and destination, be in one-hop away from between each other by creating the fake neighbours are created [7].

B) Wormhole Attack in IoT

In IoT, wormhole attack is an RPL based internal security attack where it does not happen to occur an active attack i.e., without interrupting the communication between the users that it is impossible to detect the attack [9]. There are different types of wormhole attacks in IoT devices they are Wormhole using Encapsulation, Wormhole using Out of Band Channel, Wormhole using High transmission power, Wormhole using Packet delay, Wormhole using Protocol Deviation. Table 1 show the types of wormhole attack in IoT [10].

Wormhole attack using Encapsulation: The attack mode is also called as exposed wormhole attack. The attack is used as two attacker nodes where the first attacker node is near the source which is embedded and the second attacker node is created a tunnel between the nodes near to the destination. The attacker nodes change the encapsulate packet to malicious packet and create a tunnel between them. These attacks mainly effect the parameters like packet delivery ratio, throughput and integrity of the nodes [10].

Wormhole attack using Out of Band Channel: This mode of attack of attack can be called as closed or hidden wormhole attack. They are used wired communication link. This link is having a high-quality bandwidth to diverse the two attacker nodes. These mode does not act in intermediate nodes. In the communication, it creates a route discovery with a fast response, this route is in insecure state and create a false communication [11].

Wormhole attack using High transmission Power: This mode which creates a fake shortest path, where fake shortest path has only one attacker on it. To detect the attack, it is a tough and easy to the plant the attack. The source node is in the position of the attacker node. Due to the presence of the attacker in the nodes, it changes or modify the header information and the routing table. Malicious nodes communicate in the large distances to increase the transmission power [12].

Wormhole attack using Packet relay: This attack is also known as replay-based attack. In this mode, the attack is been used as for one or more attacker node [13].

Wormhole attack using protocol Deviation: In this attack, for communication routing protocol used. These process which attack the network traffic of the network [14]. In this attack, during the communication the attacker keep an eye of the packets and capture those packets and resend the packet to the destination. This attack are used in initial step to launch the attacks [15].

IV. DETECTION APPROACHES IN WORMHOLE ATTACK

Wormhole Attack is the attacker creates a place in the network to track the information from the network and get the confidential information from the users where a tunnel or wormhole link is created in between source and destination [14,15]. For these attacks a detection mechanism is represented so that during the occurrence of attack, it can detect the attack from avoiding the node to be in malicious state [16].

A) Detection Approaches of wormhole attack in WSN

WSN is a group of networks which are spreading faster in various applications. According to the usage in various applications the need of security is needed. For this purpose, detection and prevention algorithms are introduced to keep avoid of change of malicious state of node in the network [16]. The easiest task in wormhole attack is the detection mechanism from prevention mechanism. The algorithms are illustrated well as shown below.

Geographic and temporal leashes: The algorithm which works in the form of clocks where it is loosely synchronized. In this algorithm the nodes are structures with the help of GPS tracking to track the nodes, but the process is in limited. The algorithm is a robust and straightforward [17].

LITEWORP: The approach is a lightweight process where the detection can be in quick and the packet loss is very low for this method. This approach is best countermeasure for wormhole detection [17].

Delay per hop indication (DelPHI): The identification of attack is represented in this approach by working under the principle by calculating the path time and predicted distance. The approaches works in two phase first is the route path collection and second is the sending the request like REQ [18].

Graph theoretical approach: The approach is also called as Location Aware Guard Node (LAGNs). The key establishment process took place in this approach for decoding the message from the source. If the message is been same or been suspected the attack is detected immediately [19].

Statistical Analysis of Multi-path (SAM): The approach is performed wormhole attacks in found in multipath routing. This approach which works with a term as Pmax and θ, the terms to be used when the attack rate is high [19]. Pmax is the probability of the routes and θ(theta) stands for difference between top two frequently papered links. If a wormholes attack is more than PMF (probability mass function) which is able to find out the wormhole attack rate as high or not, if it is high the frequency will also be high [20].

Secure localization: The approach uses localization method to keep away from wormhole attack. In this approach a scheme called distance-consistency-based secure location which is traps, detect from the location and detect the attack [20].

Wormhole Resistant Hybrid Technique (WRHT): The approach uses watchdog and Delphi methods. In WSN this approach that provide information during the packet drop. In each hop it finds out the delay during the full phase route. The approach is an extension version AODV routing protocol where the protocol which makes the right way to transmit the data in the network and can detect the attacks at the same [21].

Radio finger printing: It is a unique method, where the data is received from the fingerprinting devices, these signals are converted into a digital data. From this digital data that can be identified whether the attacker come to the network and detect them easily [20].

Directional Antenna: The method that can detect the wormhole attack with the help of directional antenna which connected with the nodes by using in an exact region and connect in between them. The nodes are established in pair where the information is sent and received between the nodes in the direction wise of the antenna. This approach which can easily detect the wormhole in the form of network fluctuation of the antenna [21].

B) Detection Approaches in IoT

An Internet of Things are a group of sensors and networks that are used in the daily life in form of a smart devices. It has a wide usage of applications [20]. Due to the usage in various applications the need of security is also an important role. The easiest task in wormhole attack in IoT are the detection mechanism from prevention mechanism [21]. The algorithms are illustrated well as shown below.

Hybrid approach: The approach is to detect a wormhole attack in IoT. The approach is having of two types: packet relay and encapsulation wormhole attack. the wormhole attack which has a huge number of neighbours that they create at the end of tunnel after an attack. After the occurrence of the attack the control packets are huge in number, where they create the two ends of the tunnel, even if the neighbour node is not in the transmission range [22].

High-Performance AODV routing protocol: The is AODV-HP (High-Performance Adhoc On-demand Distance Vector) routing protocol is a hybrid algorithm which is centered position. The algorithm is to detect the attack, by checking common node between the neighbors, the target hop count, and the anomaly value in the network. The algorithm is a basic and, the wormhole link is effectively separated from the concerned network due to the reason of hardware or time synchronization [23].

Location-aware Detection Scheme: The approach is attack-tolerant multi-path routing protocol where all the operation are performed in events like altering the paths, exchanging path information without additional communications.

Retrieval Number: 100.1/ijrte.A58730510121
DOI: 10.35940/ijrte.A5873.0510121
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

The attack is detected by using a location-aware wormhole detection scheme where the location information is said to be the malicious nodes by neighbouring nodes and hop level in the attack. The scheme is also used in WSN with the help of multi-routing protocol [24].

Quantum-Inspired Tabu Search (QTS) algorithm with Moving average (MA) indicator: The approach is used without any need of a hardware device and can also used in WSN. The approach is interfered as Moving Average indicator. The Quantum-inspired Tabu Search algorithm is an algorithm where the use of filter to get out the multiple combinations of MA. The approach is used for time series information are straightforward and instinctive [25].

Distributed Detection Algorithm: The approach is a wireless network coding system called DAWN, this approach is a distributed detection algorithm. The method which flows directions that are detected packets caused by a wormhole. The algorithm is a middleware or location information and create message that has the possibility of detecting the attack in exact location and stopping sharing of packets to the whole network [26].

Modified AODV: The novel approach to improve the performance of the wireless sensor nodes by overcoming the exposure of AODV [27]. These AODV have High Transmission Power type wormhole attack. The comparison on AODV and modified AODV routing protocol are the changes and improvement on the following parameters like throughput, delivery of packets, average delay [28].

V. ANALYSIS

From the survey papers, The evaluation of comparison in detection mechanisms are studied as basically the parameters used in all the algorithms as the throughput, delivery of packets and the delay of the packets [21,22,25, 27,28]. The comparison is low in the case of WSN as compared to IoT show below the table 2 the experimental results of IoT and WSN and figure 2 shows the parameter comparisons in WSN and IoT.

Table.2 Comparison results of detect mechanism in IoT and WSN [21,22,25, 27,28]

Network	Throughput	Delivery of packets	Average delay
IoT	44.6%	40%	35.5%
WSN	20.2%	27.8%	18.8%

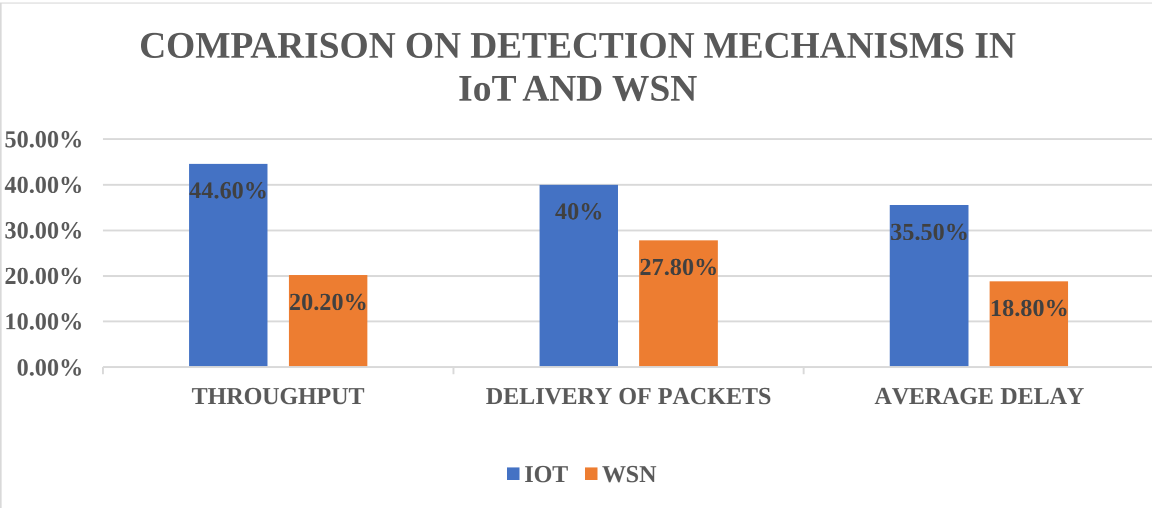

Fig.2.Parameter comparison in WSN and IoT detection mechanisms

VI. CONCLUSION

In this review, a security assault called wormhole attack is presented in both Wireless Sensor Network (WSN) and Internet of Things (IoT). The types of wormhole attack and the detection mechanism in WSN and IoT are reviewed. The wormhole attack is one of the serious threats for WSN and IoT devices by reducing sensor network performance and network traffic by creating the tunnels in between the source and destination node. In the analysis of detection mechanism by comparing with parameters of the algorithm as the throughput of IoT is 45% while in WSN is 20%, delivery of packets in IoT is 40%in WSN is 28% and average delay of IoT is 35.5% in WSN is about 18.8%. Overall result shows the performance on IoT is well and good as compared to WSN.In future, the review on other attacks like blackhole and sinkhole etc can also be incorporated in both IoT and WSN.

REFERENCES

1. M. Goyal and M. Dutta, "Intrusion Detection of Wormhole Attack in IoT: A Review," *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, 2018, pp. 1-5, doi: 10.1109/ICCSDET.2018.8821160.
2. Snehal Ajit Bhosale, S. S. Sonavane. Wormhole Attack Detection System for IoT Network: A Hybrid Approach, 16 March 2021, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-252135/v1]
3. A. Rghioui, A. Khannous, M. Bouhorma, Denial-of-service attacks on 6LoWPAN- RPL networks: threats and an intrusion detection system proposition, J. Adv. Comput. Sci. Technol. 3 (2014) 143–153, doi: 10.14419/jacst.v3i2.3321.
4. S. K. Jangir, and N. Hemrajani, "A Comprehensive Review on Detection of Wormhole Attack in MANET", in the proceedings of IEEE International Conference on ICT in Business Industry & Government, pp. 1-8, 2016.

5. A. Shrivastava and R. Dubey, “Wormhole Attack in Mobile Adhoc Network: A Survey”, International Journal of Security and Its Applications vol.9, no.7, pp.293-298, 2015.
6. M. Meghdadi, S. Ozdemir, and I. Guiler, “A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks”, IETE technical review, vol. 28, no. 2, pp. 89 – 102, 2011.
7. S. Gupta, S. Kar, and S. Dharmaraja, “WHOP: Wormhole attack detection protocol using hound packet”, in the proceedings of IEEE International Conference on Innovations in information technology, pp. 226-231, 2011. [13] S. Ji, T. Chen, S. Zhong, and S. Kak, “DAWN: Defending against Wormhole Attacks in Wireless Network Coding Systems”, in the proceedings of IEEE INFOCOM, pp. 664–672, 2014.
8. M. K. Sharma, and B. K. Joshi, “A Mitigation Technique for High Transmission Power based Wormhole Attack in Wireless Sensor Networks”, in the IEEE proceedings of International Conference on ICT in Business Industry & Government, pp. 1-6, 2016.
9. M. Bendjima, and M. Feham, “Wormhole Attack Detection in Wireless Sensor Networks”, in the proceedings of IEEE SAI Computing Conference, pp. 1319–1326, 2016.
10. M. Arai, “Reliability Improvement of Multi-Path Routing for Wireless Sensor Networks and Its Application to Wormhole Attack Avoidance”, in the proceedings of Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops, pp. 533-536, 2015.
11. T. Acharjee, P. Borah, and S. Roy, “A New Hybrid Algorithm to Eliminate Wormhole Attack in Wireless Mesh Networks”, in the proceedings of IEEE International Conference on Computational Intelligence and Communication Networks (CICN), pp. 997-1002, 2015.
12. P. Perazzo, C. Vallati, D. Varano, G. Anastasi and G. Dini, "Implementation of a Wormhole Attack Against an RPL Network: Challenges and Effects", in the proceedings of 14th Annual Conference on IEEE Wireless On-demand Network Systems and Services (WONS), pp. 95-102, 2018.
13. P.Pongle and G.Chavan, “Real-time intrusion and wormhole attack detection in the internet of things”, International Journal of Computer Applications, vol. 121, no.9, pp. 1-8, 2015.
14. Umashankar Ghugar1, and Jayaram Pradhan2, A Review on Wormhole Attacks in Wireless Sensor Networks, International Journal of Information Communication Technology and Digital Convergence (2019).
15. M.G. Zapata, Secure Ad hoc On-Demand Distance Vector Routing, ACM SIGMOBILE Mobile Computing and Communications Review. Jun, (2002), vol, 6(3), pp.106-107.
16. C. Zhu, M. J. Lee, T. Saadaw, RTT-Based Optimal Waiting Time For Best Route Selection In Ad Hoc Routing Protocols, IEEE Military Communication Conference, Vol.2 Oct, (2003), pp1054-1059.
17. K.U.R Khan, A.V. Reddy, R.U. Zaman, K.A Reddy, T.S Harsha, An Efficient DSDV Routing Protocol for Wireless Mobile Ad Hoc Networks and its Performance Comparison, Second UKSIM European Symposium on Computer Modeling and Simulation, India, (2008), pp. 506-511.
18. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A Survey Of Routing Attacks In Mobile Ad Hoc Networks, IEEE Wireless Communication, vol. 14(5), October, (2007).
19. A. Verma and N. Bhardwaj, A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol. International Journal of Future Generation Communication and Networking, vol. 9(4), (2016), pp. 161-170.
20. U. Ghugar, J. Pradhan, Intrusion Detection System in Wireless Sensor Networks for Wormhole Attack Using Trust-Based System, Handbook of Research on Information Security in Biomedical Signal Processing, IGI Global, (2018).
21. E. Kaffashi, A. Mousavi, H. Rahvard, A new attack on link-state database in open shortest path first routing protocol. Journal of Electrical and Electronic Engineering, (2015); vol. 3(2-1), pp. 39-45.
22. L. Hu, D. Evans, Using Directional Antennas to Prevent Wormhole Attacks, 14 Proceedings of the 11th Network and Distributed System Security Symposium, pp. (2003).
23. Y. C. Hu, A. Perrig, D. B. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks, inProc. of IEEE -INFOCOM, (2003), pp. 1976-1986, vol.3.
24. Y. Singh, A.Khatkar, P.Rani, Wormhole Attack Avoidance Technique in Mobile Adhoc Networks, Third International Conference on Advanced Computing & Communication Technologies, Rohtak, 6-7 April (2013).
25. P.Nayak, A.Sahay, Y.Pandey, Detection and Prevention of Wormhole Attacks in MANETs using Detection Packet”, International Journal of Scientific & Engineering Research, vol. 4 (6), June-(2013).
26. A.Patel, N.Patel, R.Patel, Defending Against Wormhole Attack in MANET, Fifth International Conference on Communication Systems and Network Technologies, (2015), pp. 674-678.
27. R.Singh, J. Singh, R. Singh, WHRT: A Hybrid Technique For Detecting Of Wormhole Attack in Wireless Sensor Networks, Mobile Information Systems, Hindawi Publishing Corporation, vol. (2016), Article ID8354930, pp. 1-13.
28. Pavan Pongle, Gurunath Chavan, “A survey: Attacks on RPL and 6LoWPAN in IoT”, International Conference on Pervasive Computing (ICPC) IEEE, 2015.
29. Parvathy K, S. Rajalakshmi, "A Review on Network Layer Attacks in Wireless Sensor Networks," International Journal of Computer Sciences and Engineering, Vol.9, Issue.3, pp.45-48, 2021.

AUTHORS PROFILE

Parvathy.K, is an Assistant Professor in Department of Computer Science and Engineering at Sri Ramakrishna Institute of Technology Coimbatore. She completed her BE CSE from Sri Ramakrishna Engineering College Coimbatore at the year 2015 and ME CSE from Sri Ramakrishna Engineering College Coimbatore at the year 2017.she is pursuing PhD from Karunya Institute of Technology and Sciences (Deemed to be University) Coimbatore. Her area of interest are internet of things, wireless sensor networks and network security etc.